



Infrastructure Protection Act - Guide for Responsible Person

As at Sep 2025

Every care has been taken to ensure the accuracy of the information contained in this guide at the time of publication. Please refer to the Infrastructure Protection Act and the related Subsidiary Legislations for the most up-to-date information on the Act.

CONTENTS



INTRODUCTION	5
Objectives of this Document	5
Structure of this Document	5
CHAPTER 1: Security-By-Design Framework and the Infrastructure Protection Act	6
What is Security-By-Design?	6
Who oversees the Security-By Design process?	6
How does the Security-by-Design process work?	6
What buildings are required to undergo the Security-by-Design process under the Infrastructure Protection Act?	7
CHAPTER 2: Management of Critical Physical Infrastructure under the Infrastructure Protection Act	8
Responsibility for security of Critical Physical Infrastructure under the Infrastructure Protection Act	8
Identification of Critical Physical Infrastructure.....	9
Designation of Critical Physical Infrastructure as Special Development/Special Infrastructure	9
Requirement to submit Security Plan for approval	9
Requirement to implement and maintain measures in Approved Security Plan.....	11
Notification of change in Responsible Person of Critical Physical Infrastructure	12
Cessation of Critical Physical Infrastructure as Special Development/Special Infrastructure	12
CHAPTER 3: Management of Large/Iconic Infrastructure under the Infrastructure Protection Act	13
Responsibility for security of large/iconic infrastructure under the Infrastructure Protection Act	13
Identification of large/iconic infrastructure.....	13
Designation of large/iconic infrastructure as Special Development/Special Infrastructure	14
Requirement to submit Security Plan for Approval	15
Requirement to implement and maintain measures in Approved Security Plan.....	16
Notification of change of RP of large/iconic infrastructure	17
Cessation of large/iconic infrastructure as Special Developments/Special Infrastructure	17
CHAPTER 4: Security-by-Design Technical Guide	18
Security-by-Design Overview and Timeline	18
Application for Commissioner of Infrastructure Protection's Approval of Security Plan.....	19



Application for Commissioner's Approval of Amendment of Approved Security Plan before the completion of specified works..... 24

Supervise implementation of security measures during specified works..... 24

Documentation25

Assess changes to Approved Security Plan..... 25

Application for Commissioner's Approval of Certificate of Works Completion25

Audits and Enforcement.....25

List of Abbreviations.....26

Annexes.....27

Annex A – Competent Person (Security/Blast)28

Annex B – Key Building Design Considerations.....34

Annex C – Requirements for Threat, Vulnerability and Risk Assessment (TVRA)39

Annex D – Requirements for Blast Effect Analysis (BEA)/Structural Resiliency Study (SRS).45

Annex E – Requirements for Security Protection Plan (SPP)56

Annex F – Documentary Submission Before and During Construction.....68

Annex G – Amendments to Approved Security Plan.....69

Annex H – Requirements for Approval of Certificate of Works Completion.....75

Annex I – Information Security80

Annex J – Requirements for Purpose-Built Shelter Report.....86



DOCUMENT CHANGE RECORD

Date	Version	Change Details
Sep 2020	v1.1	<ol style="list-style-type: none"> 1. Para 75 - 81 2. Annex B para 4.1
Apr 2021	V1.2	<ol style="list-style-type: none"> 1. Annex D1 of Annex D 2. Appendix of Annex E
Sep 2025	V1.3	<ol style="list-style-type: none"> 1. Main Guide <ol style="list-style-type: none"> a. Requirement for Workplace Shelter and Purpose-built Shelter 2. Annex A <ol style="list-style-type: none"> a. Responsible Person Duties b. Annex A1 – Working with CPs to manage SBD projects [New] 3. Annex B <ol style="list-style-type: none"> a. Workplace Shelter [New] b. Force entry resistance [New] 4. Annex C <ol style="list-style-type: none"> a. Critical function [New] b. Security objective [New] c. Appendix – TVRA Outline Template [New] 5. Annex D <ol style="list-style-type: none"> a. Single-Degree-Of-Freedom (SDOF) requirement b. Finite Element Analysis (FEA) [New] c. Table C – Summary of Ground Shock Analysis Results [New] d. Table E – Details of Physical Hardening/Non-Hardening Measures 6. Annex E <ol style="list-style-type: none"> a. Structural/Physical Measure Table – Requirements on Ground Shock Protection, Vehicle Speed Analysis, Fence line and Force Entry b. Technological Measures/Security Systems - Requirements on Video Surveillance System, Lighting, Access Control System, Intrusion Detection Systems, Security Screening Systems, Electronic Key Management System and Security Integrated Platform [New] c. Workplace Shelter - Requirements on Workplace Shelter [New] d. Articulation of Final Residual Risk – Requirements on final residual risk 7. Annex F

		<ul style="list-style-type: none">a. Changes to the documents to be submitted during construction <ul style="list-style-type: none">8. Annex G<ul style="list-style-type: none">a. Amendments to approved security planb. Appendix 1 <i>[New]</i>9. Annex H<ul style="list-style-type: none">a. Additional requirements <i>[New]</i>10. Annex I <i>[New]</i>11. Annex J <i>[New]</i>
--	--	--



INTRODUCTION

1. Global terrorism is on the rise and Singapore is facing our highest threat of terror in recent years. Buildings which house essential services, or are iconic, or with high human traffic, could be targeted by terrorists, with the intent of disrupting such services or inflicting mass casualties.
2. Building security is therefore a key part of our strategy to protect Singapore from terrorist attacks. The Infrastructure Protection Act (**IPA**) establishes a clear regulatory framework to systematically protect Singapore's infrastructure where a successful attack would have disproportionate harm on the public and Singapore. The IPA also provides more transparency and clarity about building security requirements and processes for building owners and developers.

Objectives of this Document

3. This document sets out statutory requirements for building security mandated under the IPA, which was operationalised on 18 December 2018. It seeks to inform owners of or persons responsible for Special Developments (**SDs**) and Special Infrastructures (**SIs**) (also known as "Responsible Persons" (**RPs**)) designated under the IPA of the following:
 - a. MHA's Security-By-Design (**SBD**) framework mandated under the IPA and its underlying concepts;
 - b. Types of developments/infrastructure that will be subjected to MHA's SBD framework, and the procedures by which they will be designated; and,
 - c. Regulatory requirements for the submission and approval of Security Plans for SDs and SIs through MHA's SBD framework.
4. Revisions to this document will be issued from time to time. Please check our [website](#) for the latest version. If you have any comment or feedback, please write to us via go.gov.sg/askcps.

Structure of this Document

5. This document is divided into the following chapters:

Chapter 1	SBD Framework and the IPA
Chapter 2	Management of Critical Physical Infrastructure under the IPA
Chapter 3	Management of Large/Iconic Infrastructure under the IPA
Chapter 4	SBD Technical Guide

CHAPTER 1: Security-by-Design Framework and the Infrastructure Protection Act

What is Security-by-Design?

6. The IPA ensures that Critical Physical Infrastructure (CPI), as well as large/iconic buildings are designed with security in mind. In the past decade, MHA has been working with owners of such key infrastructure to take security into account upfront in the development process, by integrating security measures into the building design. This process is known as Security-by-Design (**SBD**).
7. The key benefit of SBD is that security is effectively incorporated into the building without overly compromising other factors such as the design concept, form and function of the building. It is generally more cost-effective because good design can reduce or even eliminate the need for some security measures. It also avoids costly retrofitting later on.

Who oversees the SBD process?

8. The Commissioner of Infrastructure Protection will oversee the SBD process under the IPA and is appointed by the Minister for Home Affairs. The Commissioner is supported by the Centre for Protective Security (**CPS**).

How does the SBD process work?

9. Firstly, a security and/or blast consultant should be brought on board by the RP to identify the risks and vulnerabilities of a building, and to develop the necessary security measures to mitigate the risks. The security and/or blast consultant must be approved by the Commissioner of Infrastructure Protection as a Competent Person (**CP**) for the project.
10. Secondly, security measures should be proposed by the CP to mitigate the relevant security risks as part of the Security Plan to be submitted to the Commissioner for approval. A **localised** and **outcome-based** approach is used to determine the appropriate security measures.
 - a. **Localised** – SBD process is risk-calibrated and focused. Protection measures are prioritised and focused on the areas of higher risk.
 - b. **Outcome-based** – SBD process is flexible. There are different ways to achieve the same security outcome. CPS generally does not prescribe specific risk methodologies or standards, or security measures.
11. Thirdly, CPS works together with the RP and CP to progressively review the various assessment and security reports, in consultation with the respective Government

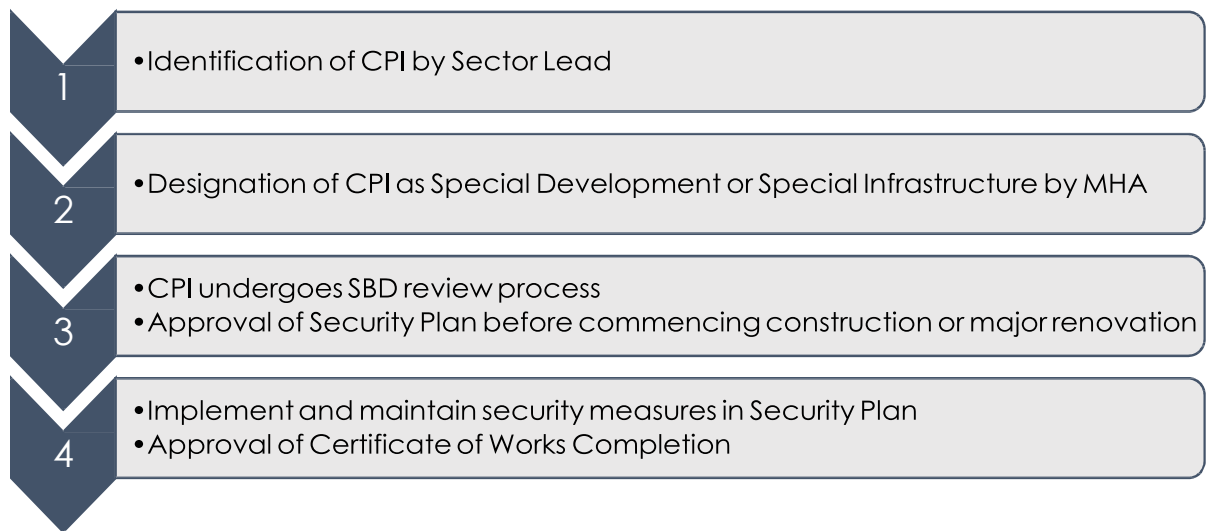
agencies having regulatory oversight or statutory responsibility for the sector (“Sector Lead Agencies”). This is to ensure that the infrastructure is adequately protected against the identified threat scenarios before formal submission of the Security Plan. This is done concurrently with the rest of the detailed design works for the building.

12. Once the Commissioner has approved the security plan for that infrastructure, building works for that infrastructure may then commence (assuming Provisional or Written Permission from URA has been obtained). All security measures stated in the approved Security Plan must be implemented and maintained.
13. The full details of the SBD process can be found in “[Chapter 4: SBD Technical Guide](#)”.

What buildings are required to undergo the SBD process under the IPA?

14. MHA will designate two groups of buildings to undergo the SBD process:
 - a. First, CPIs which are vital to the delivery of essential services such as water, power and transport; and
 - b. Second, large or iconic buildings which face a higher level of threat either due to high public footfall, or because of their prominence or symbolic significance.

CHAPTER 2: Management of Critical Physical Infrastructure under the IPA



Responsibility for security of CPI under the IPA

15. Critical Physical Infrastructures (**CPIs**) are physical infrastructure and assets that are vital for the continued delivery of the essential services that Singapore relies on. The loss or compromise of such infrastructure would lead to a debilitating impact on security, economy or public health and safety. CPIs underpin the functioning of Singapore's society and economy, by enabling the provision of essential services such as food, water, medical care, energy, communications, transportation and banking.
16. A national unity of effort is needed to strengthen the security of CPIs against physical threats. Although the Government has a role in the protection of CPIs, owners/operators of CPIs will also need to be responsible for the security of their own assets and the continuity of their businesses. These efforts should seek to reduce vulnerabilities, minimise consequences, identify and mitigate threats, and hasten response and recovery efforts related to CPIs.
17. The person responsible for ensuring that security requirements under the IPA are met is determined based on the legal entity having control and management of the premise the CPI is in. This will generally be the owner of the CPI (also known as "Responsible Person" (**RP**)). Where the CPI has more than one owner, all its owners are collectively treated as the RP.
18. However, in cases where the CPI is housed in a premise that is not owned by the owner of that CPI (e.g. leased data centres), the RP will be the owner of the CPI and not the premise owner.

Identification of CPI

19. CPIs are primarily identified by the Sector Lead Agencies, in consultation with the RP for the CPI.
20. Companies providing essential services should regularly consult their respective Sector Lead Agencies on whether there is any planned developments or existing infrastructure would be identified as a CPI. Failure to identify a CPI early may result in downstream delays to its development timeline, if security considerations cannot be factored into the SBD process during the building design phase.

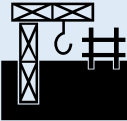
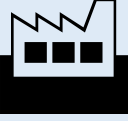
Designation of CPI as Special Development/Special Infrastructure

21. MHA will inform the RP of the CPI in writing that their CPI will be designated as a Special Development (**SD**) (if the CPI has not been built or is in the process of being built), or as a Special Infrastructure (**SI**) (if the CPI has already been built). This applies to all existing CPIs and new CPIs identified in the future. For security reasons, information on which buildings are CPIs and designated as SDs or SIs is restricted to RPs, Sector Lead Agencies and security agencies.
22. Where the premise of a CPI is solely owned by the RP, the entire CPI's premise will be designated as a SD/SI as a whole. This will allow the security of the entire CPI to be considered holistically.
23. Where the CPI only occupies part of a larger premise that is not solely owned by the RP (e.g., a data centre in a commercial tenanted facility), only the part of the premise that the CPI occupies will be designated.
24. In the rare scenario where there are two or more CPIs sharing the same premise, MHA will work together with the relevant RPs to determine the appropriate boundaries that would be consistent with the extent of management and control each RP has for their CPI. Similarly, for large-scale CPIs that will be constructed over multiple phases, MHA will work with the relevant RP to phase and align the designation of such CPIs as SD/SI to the various stages of development where possible, based on the extent of management and control each RP has for their CPI.

Requirement to submit Security Plan for approval

25. Once designated as a SD/SI, it will be a **legal requirement for the RP to submit a Security Plan to the Commissioner of Infrastructure Protection for approval, before specified works can be carried out:**
 - a. CPIs that are yet to be built or in the midst of construction (designated as SDs) will be required to obtain Commissioner's approval for the Security Plan before commencing construction;

- b. Existing CPIs (designated as SIs) will be required to obtain Commissioner's approval for the Security Plan before commencing any major renovation works.

 <p>Critical Physical Infrastructure yet to be built / in the midst of construction</p>	 <p>Existing Critical Physical Infrastructure</p>
<ul style="list-style-type: none"> • Designated as "Special Developments" • Obtain approval for Security Plan before starting construction works* <p><i>*Construction works refer to any works for or affecting the foundation, retaining structure, substructure or superstructure of any building/structure (whether temporary or permanent) to be constructed.</i></p>	<ul style="list-style-type: none"> • Designated as "Special Infrastructure" • Obtain approval for Security Plan before starting any major renovation works, including any extension to the existing building/structure • Major renovation works refer to <ol style="list-style-type: none"> i. In the case of any part of a building/structure containing a critical asset, or is a public place or is accessible to vehicles or vessels, any alteration, extension, repair, dismantling or demolition works carried out to the structure or glazing of that part ii. Any installation or relocation of a critical asset in the premises iii. Any alteration, extension, dismantling or demolition works affecting the perimeter of the premises <p><i>[Major renovation works generally do not include insignificant or superficial building works such as painting, erection of internal partitions, landscaping works.]</i></p>

- 26. In instances of major renovations, the Security Plan may be required to cover areas outside of the proposed renovation works, so that security risks to the designated premises may be addressed adequately. The scope of such security measures will be based on practical considerations, such as to install or upgrade access control or video surveillance systems.
- 27. Further details on the Security Plan approval process may be found in "[Chapter 4: SBD Technical Guide](#)".
- 28. Carrying out, causing or allowing the carrying out of any specified works for a SD or SI, without approval of Security Plan by the Commissioner is an offence under the IPA. If convicted, the penalty is a fine not exceeding \$200,000 or imprisonment for a term not exceeding 2 years, or both.



29. In addition, the Commissioner may direct the RP to stop any specified works and take actions to comply with the requirement to submit a Security Plan for approval.
30. The requirement to obtain Commissioner's approval for the Security Plan before starting specified works is also incorporated in URA's conditions when applying for Provisional or Written Permission to carry out works.
31. **RPs should inform CPS of upcoming specified works as early as possible**, such as during the project's concept design stage. The earlier CPS is brought on board, the more support CPS will be able to provide during the conduct of the risk assessments and development of the Security Plan. Such support includes advice on the scope of the security review, site selection and the security considerations based on the preliminary design concept of the building.

Requirement to implement and maintain measures in Approved Security Plan

32. After the Commissioner of Infrastructure Protection approves the Security Plan, works can begin (assuming Provisional or Written Permission from URA has been obtained). The security measures in the Approved Security Plan (ASP) must be implemented. The ASP will specify the implementation schedule for security measures:
 - a. **Security measures that are required to be implemented before or upon the completion of specified works.**

Upon the completion of specified works, the RP is required to submit a Certificate of Works Completion (CWC) to the Commissioner for approval. The CWC certifies that the required security measures have been implemented by the time specified works are completed.

 - i. If the specified works require a Temporary Occupation Permit (TOP) or Certificate of Statutory Completion (CSC) from the Building and Construction Authority (BCA), these cannot be obtained without a CWC.
 - ii. If the specified works do not require a TOP or CSC from BCA, the CWC must be submitted within **10 working days** after the completion of specified works.
 - b. **Security measures that are required to be implemented after the Commissioner's approval of the CWC.**

The remaining security measures must be implemented in accordance with the schedule set out in the ASP.
33. After the CWC is approved, a SD becomes a SI and the ASP of the SD becomes the ASP of the SI. The RP must then maintain every security measure that is implemented under the ASP, in order to ensure the operational effectiveness of every security measure.

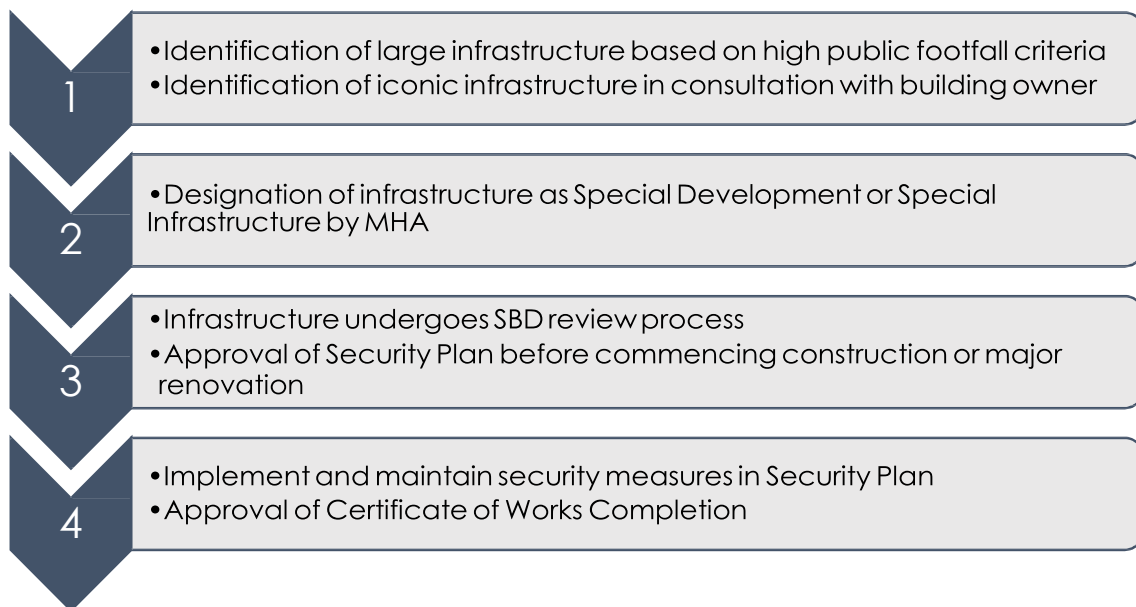
34. Further details on the CWC approval process and requirements may be found in "[Chapter 4: SBD Technical Guide](#)".
35. Failure to implement or maintain every security measure stated in an ASP is an offence under the IPA. If convicted, the penalty is a fine not exceeding \$20,000 or imprisonment for a term not exceeding 2 years, or both. In the case of a continuing offence, a further fine not exceeding \$1,000 for every day during which the offence continues after conviction will be imposed.
36. In addition, the Commissioner may direct the RP to take actions to rectify non-compliance with the ASP.

Notification of change in RP of CPI

37. Where there is a change in the legal ownership/occupation of a CPI that is designated as a SD or SI, the person who was the original RP before the change in ownership/occupation is required to inform CPS within seven days of the change in ownership, through the submission of a notification form found on our [website](#).

Cessation of CPI as Special Development/Special Infrastructure

38. A CPI will cease to be a SD or SI when the Minister cancels its designation by written notice to the RP. This may happen when the premise is demolished, decommissioned or the CPI is relocated. The RP of the SD or SI should inform CPS once there are plans to demolish, decommission or relocate the CPI via go.gov.sg/askcps.



Responsibility for security of large/iconic infrastructure under the IPA

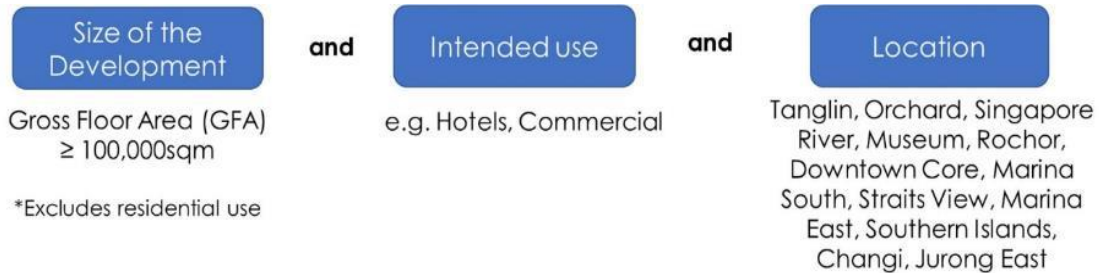
39. Building owners have the primary responsibility for protecting their own buildings, including a duty of care to take steps to protect the people who work, use, or visit their building from a range of foreseeable threats, including terrorism. The reputation of building owners will suffer serious and permanent damage if priority is not given to protecting people against attack. Reputational damage can also have a significant impact on businesses' finances.
40. For certain buildings, the risk and impact of an attack are much more significant. Large or iconic buildings face a higher level of threat due to high public footfall, or their prominence or symbolic significance. In these cases, it is in the interest of the public to ensure that appropriate security measures are put in place to safeguard lives and property.
41. Under the IPA, the owners of large/iconic infrastructure (also known as "Responsible Persons" (**RP**s)) will be responsible for ensuring that security requirements under the IPA are met. This is determined based on the legal entity having control and management of the infrastructure. Where there is more than one owner, all the owners are collectively treated as the RP.

Identification of large/iconic infrastructure

42. Large buildings will primarily be identified based on the following three criteria



which serve as objective proxies for a development's capacity to attract large crowds due to high public footfall – namely the size of the development (in terms of gross floor area), its intended use (based on URA's approved use) and its location (based on URA's Planning Areas).



43. Developers and building owners who are unsure whether their buildings meet the criteria may contact CPS for clarification via go.gov.sg/askcps.
44. Other developments/buildings that do not meet the criteria in para 42 may also be designated by the Minister for Home Affairs as Special Developments (SDs) or Special Infrastructures (SIs). This includes large/iconic developments/buildings, such as those of symbolic significance to Singapore. Such buildings will be identified as early as possible in the pre-development phase, in consultation with the developer or building owner.

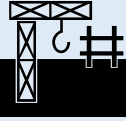

Designation of large/iconic infrastructure as Special Development/ Special Infrastructure

45. All large developments that are yet to be built and meet the high public footfall criteria, are designated as SDs under the IPA. This will include all new developments that start/proposed to start construction on or after 1 January 2020.
46. For existing large buildings that meet the high public footfall criteria, they will also generally be designated as SIs. MHA will engage building owners and assess the need for security measures, taking into consideration the buildings' actual land use and profile. MHA will inform building owners of the designation in writing.
47. MHA may also designate yet to be built and existing developments that do not meet the high public footfall criteria, but are iconic, as SDs/SIs. Developers will be informed of MHA's intention to designate such developments in writing, as early as possible.
48. Where there are multiple RPs for different parts of the SD or SI, MHA will work together with all relevant parties to determine the appropriate boundaries that would be consistent with the extent of management and control each RP has for their part of the building.

Requirement to submit Security Plan for Approval

49. Once designated as a SD or SI, it will be a **legal requirement for the RP of large/ iconic buildings to submit a Security Plan to the Commissioner of Infrastructure Protection for approval, before specified works can be carried out:**

- a. Developments that are yet to be built or in the midst of construction (designated as SDs) will be required to obtain Commissioner’s approval for the Security Plan before commencing construction;
- b. Existing buildings (designated as SIs) will be required to obtain Commissioner’s approval for the Security Plan before commencing any major renovation works.

 <p>Large/Iconic Developments yet to be built/ in the midst of construction</p>	 <p>Existing Large/Iconic Buildings</p>
<ul style="list-style-type: none"> • Designated as “Special Developments” • Obtain approval for Security Plan before starting construction works* <p><i>*Construction works refer to any works for or affecting the foundation, retaining structure, substructure or superstructure of any building/structure (whether temporary or permanent) to be constructed.</i></p>	<ul style="list-style-type: none"> • Designated as “Special Infrastructure” • Obtain approval for Security Plan before starting any major renovation works, including any extension to the existing building/structure • Major renovation works refer to <ul style="list-style-type: none"> i. In the case of any part of a building/structure containing a critical asset, or is a public place or is accessible to vehicles or vessels, any alteration, extension, repair, dismantling or demolition works carried out to the structure or glazing of that part ii. Any alteration, extension, dismantling or demolition works affecting the perimeter of the premises <p><i>[Major renovation works generally do not include insignificant or superficial building works such as painting, erection of internal partitions, landscaping works.]</i></p>

50. In instances of major renovations, the Security Plan may be required to cover areas outside of the specified works, so that security risks to the designated premises may be addressed adequately. The scope of such security measures



will be based on practical considerations, such as to install or upgrade access control or video surveillance systems.

51. Further details on the Security Plan approval process may be found in "[Chapter 4: SBD Technical Guide](#)".
52. Carrying out, causing or allowing the carrying out of any specified works for a SD or SI, without the approval of Security Plan by the Commissioner is an offence under the IPA. If convicted, the penalty is a fine not exceeding \$200,000 or imprisonment for a term not exceeding 2 years, or both.
53. In addition, the Commissioner may direct the RP to stop any specified works and take actions to comply with the requirement to submit a Security Plan for approval.
54. The requirement to obtain Commissioner's approval for the Security Plan before starting specified works is also incorporated in URA's conditions when applying for Provisional or Written Permission to carry out works.
55. **RPs should inform CPS of upcoming specified works as early as possible** (such as during the project's concept design development stage). The earlier CPS is brought onboard, the more support CPS will be able to provide during the conduct of the risk assessments and development of the Security Plan. Such support includes advice on the scope of the security review, site selection and the security considerations based on the preliminary design concept of the building.

Requirement to implement and maintain measures in Approved Security Plan

56. After the Commissioner of Infrastructure Protection approves the Security Plan, works can begin (assuming Provisional or Written Permission from URA has been obtained). The security measures in the Approved Security Plan (ASP) must be implemented. The ASP will specify the implementation schedule of security measures:
 - a. **Security measures that are required to be implemented before or upon the completion of specified works.**

Upon the completion of specified works, the RP is required to submit a Certificate of Works Completion (CWC) to the Commissioner for approval. The CWC certifies that the required security measures have been implemented by the time specified works are completed.

 - i. If the specified works require a Temporary Occupation Permit (TOP) or Certificate of Statutory Completion (CSC) from the Building and Construction Authority (BCA), these cannot be obtained without a CWC.
 - ii. If the specified works do not require a TOP or CSC from BCA, the CWC

must be submitted within **10 working days** after the completion of specified works.

b. **Security measures that are required to be implemented after the Commissioner's approval of the CWC.**

The remaining security measures must be implemented in accordance with the schedule set out in the ASP.

57. After the CWC is approved, a SD becomes a SI and the ASP of the SD becomes the ASP of the SI. The RP must then maintain every security measure that is stated in the ASP, in order to ensure the operational effectiveness of every security measure.
58. Further details on the CWC approval process and requirements may be found in "Chapter 4: SBD Technical Guide".
59. Failing to implement or maintain every security measure stated in an ASP is an offence under the IPA. If convicted, the penalty is a fine not exceeding \$20,000 or imprisonment for a term not exceeding 2 years, or both. In the case of a continuing offence, a further fine not exceeding \$1,000 for every day during which the offence continues after conviction will be imposed.
60. In addition, the Commissioner may direct the RP to take actions to rectify non-compliance with the ASP.

Notification of change of RP of large/iconic infrastructure

61. Where there is a change in the legal ownership of a large/iconic building that is designated as a SD or SI, the original RP before the change in ownership is required to inform CPS within seven days of the change in ownership, through the submission of a notification form found on our [website](#).

Cessation of large/iconic infrastructure as Special Developments /Special Infrastructure

62. A development or building will cease to be a SD or SI when the Minister cancels its designation by written notice to the RP. This may happen when the premise is demolished or decommissioned. The RP of the SD or SI should inform CPS once there are plans to demolish or decommission the development or building via go.gov.sg/askcps.

Security-by-Design (SBD) Overview and Timeline

63. The SBD review process adopts a risk management approach. Risk management is the process of:

- a. identifying critical assets to be protected and their vulnerabilities;
- b. identifying threat scenarios; and,
- c. assessing the risks and prioritising the mitigation measures to reduce the risks to an acceptable level.

64. The typical SBD timeline is shown in Fig. 1 below.

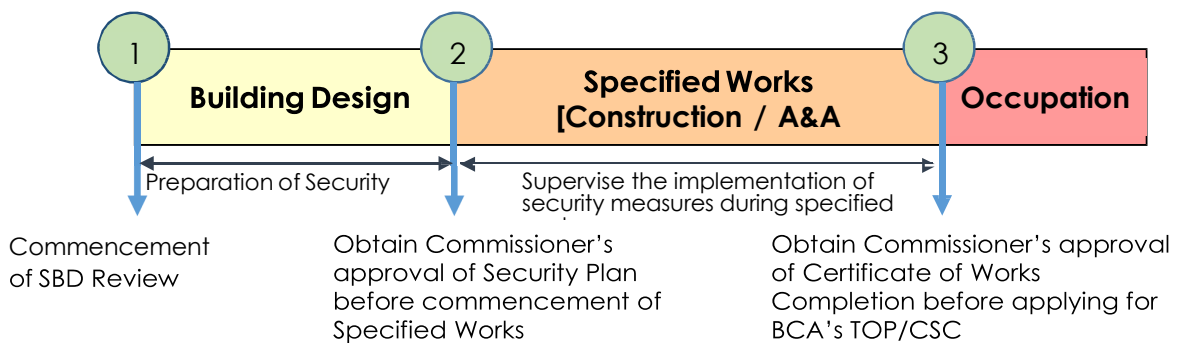


Fig. 1 Submission timeline

65. The SBD process is carried out concurrently with the detailed building design. As the SBD process is outcome-based, the experience with past projects has shown that the SBD process can be integrated seamlessly with the building design process, especially if security considerations are incorporated early into the design. Based on previous projects, generally the preparation and approval of Security Plan under the SBD process will take about 9 to 12 months to complete¹, in parallel with the other design works for that infrastructure.

66. In general, CPS will take about **15 working days** to process each iteration of submitted replies and reports (see para 73 for the reports to be submitted). To avoid delays to the SBD process, the RP should respond to CPS's clarifications within **10 working days**. The RP will have to inform CPS if extension of time is required. The number of iterations taken for each report depends on the quality and standard of the report submitted. After CPS has cleared all the reports, the RP may submit an application to seek the Commissioner of Infrastructure Protection's approval for Security Plan. CPS requires **20 working days** to process the approval application before issuing the approval letter.

¹ For projects that need to develop structural hardening measures. For developments that do not need to develop structural hardening measures, the SBD process can be shorter. Excludes time taken to hire security/blast consultants.

Application for Commissioner of Infrastructure Protection's Approval of Security Plan

67. It is a legal requirement for the RP to obtain the Commissioner of Infrastructure Protection's approval for the Security Plan before commencing Specified Works. The following steps set out the application workflow.

Step 1: Security Clearance

68. All personnel involved in the SBD review must undergo security screening by MHA, before they can access sensitive project information. This will include the Competent Person (**CP**) (described in Step 2) and may also include senior management and project managers. Due to the confidential nature of the review, the RP should safeguard information related to the review process and limit the number of personnel involved on a strict need-to-know basis.

Step 2: Appointment of Security and/or Blast consultant as Competent Person

69. Security Plans submitted to the Commissioner of Infrastructure Protection must be prepared by a security and/or blast consultant that is approved by the Commissioner to be a CP. Please refer to [Annex A](#) for the requirements for the CP. The role of the CP is to develop effective security solutions against a list of threats provided by MHA, in order to meet the security objectives set out for the Special Development (SD)/Special Infrastructure (SI). This will involve carrying out risk assessments and integrating security planning and solutions into the building's overall design, by working closely with the other project consultants to achieve optimal security solutions. RPs should identify a suitable security and/or blast consultant and submit an application for the approval of CP to CPS **early** in the concept design development stage of the SD/SI. RPs engaging CPs who are foreigners, would also need to ensure that they comply with the regulations under the Employment of Foreign Manpower Act. Please refer to Appendix A-1 for pointers to help RP to manage CPs in SBD projects.

70. The CP will be required to apply evidence-based, tested, and internationally proven methodologies on possible threat scenarios to derive the risk factors. The CP is also responsible for incorporating the RP's inputs, including constraints, preferences, operational/functional requirements, decisions made, etc., into the required reports before they are submitted for CPS's review.

Who may be appointed as a CP?

- CP may be commercial or in-house security and/or blast consultants. The CP (Security) shall be the main security consultant responsible for the SBD review. If blast-related assessments are required, the RP shall appoint a CP (Blast) to carry out the blast-related assessments, who may or may not be the same CP (Security).
- The Commissioner will make an assessment of the CP for each project based on, but not limited to, the person's relevant qualifications, past experience with SBD projects and the nature of the project.

- CP needs to be approved by the Commissioner of Infrastructure Protection on a per-project basis as some projects may require special expertise or may be sensitive in nature.

How should RP assess and select Security and/or Blast consultants?

- RPs should select a security and/or blast consultant based on the requirements and scope of their project. RPs may consider the following factors in assessing and selecting security/blast consultants:
 - Education, qualification, skills and experience
 - Referee reports
 - Professional association and affiliations
 - Previous experience conducting security reviews
 - Relevant subject matter knowledge
 - Impartiality of advice (consider any commercial affiliations)
 - Published professional work

Step 3: Arrange for SBD Kick-off Meeting

71. RPs may arrange a kick-off meeting with CPS to share about the project and for CPS to share key requirements².
72. The RP will be informed of the assessed risk profile during the designation of the SD/SI. Based on the risk profile, the RP will determine the security objectives specific to the SD/SI and that will set the direction of the development of the Security Plan.
 - a. In the case of a CPI, this will involve identifying the critical assets and the minimum service level. In addition, the RP will also determine whether a Workplace Shelter³ or Purpose-built Shelter⁴ is required.
 - b. In the case of large/iconic infrastructure, this will involve identifying areas of mass congregation that need to be protected.

What are Critical Assets?

- Critical Assets are facilities, systems or equipment which, if damaged or destroyed, may have a debilitating impact on the functioning of the premises. For example, these may include power generators, Air Handling Units (AHUs), telecommunications switches, etc.
- RPs are responsible for identifying and assessing critical assets for their SDs/SIs. In the case of CIs, RPs should also consult the relevant Sector Lead Agencies regulating or overseeing the CI when identifying the Critical Assets for the CI.

² Key requirements include SBD review process and timeline, checklist for the reports, RP's roles and responsibilities, CP's roles and responsibilities, potential red flags and pathways for escalation.

³ Workplace Shelter are hardened spaces where the essential personnel could seek temporary refuge from the weapon effects. Generally, Workplace Shelters are co-located within a critical asset room and sited at a location that is near where the essential personnel are expected to be stationed.

⁴ Purpose-built Shelters are designed for continued 24/7 operations throughout the high-risk period i.e., provide a safe area for personnel to work or rest without the burden of wearing the individual personnel protective equipment.

Step 4: Submission of Security Plan

73. The CP will have to prepare up to four reports – Threats, Vulnerability and Risk Assessment (TVRA), Blast Effect Analysis (BEA), Structural Resiliency Study (SRS) and Security Protection Plan (SPP). These reports are collectively referred to as the Security Plan in the IPA. An additional Shelter Report is required to be submitted as part of the Security Plan for projects that have Purpose-built Shelters.

TVRA and BEA reports

- a. When the building's design and structural systems are being developed, the CP shall work closely with the relevant persons to incorporate sensible security design practices to minimise security risks to the critical assets. Please refer to [Annex B](#) for a description of Key Building Design Considerations. The CP will have to consider the functional needs of the building and the operational requirements of the RP.
- b. The CP shall be required to carry out a risk assessment of the building to determine the risks to the critical assets, with the findings included in the TVRA report. The TVRA report should consist of an introduction of the Facility, including the purpose, nature of its business and how it functions, a list of critical assets supporting the operations, its location and layout, existing/baseline security measures and its ranked security objectives. Please refer to [Annex C](#) for requirements for the TVRA report.
- c. Where the vulnerabilities of structural elements against explosive loads need to be studied in order to determine the risks, the CP will identify the affected structural elements and conduct a BEA to determine their adequacies. Please refer to [Annex D](#) for requirements for the BEA report. BEA reports are not required for SDs or SIs that do not need structural hardening.
- d. The TVRA and BEA reports have to be prepared in consultation with the RP and submitted concurrently to CPS. After the submission of any report, the CP will support the RP by providing any necessary clarifications and justifications. The review may be carried out over a few iterations and the RP has to go through the CP's reports, clarifications and agree on the risk assessment and the prioritisation of critical assets to be protected based on the risk scoring.
- e. The CP is to update the reports with the necessary amendments, clarifications and supporting information after the reports have been accepted.

SRS and SPP reports

- a. The CP shall recommend in the SPP a comprehensive suite of security measures to address **all** the risks, as determined from the risk assessment, to fulfil the stated security outcome, with the exact combination of structural/physical, operational and technological measures to be calibrated according to the risks posed by the various threat scenarios and the criticality of the assets in question. The CP shall:

- i. Rank the recommended security measures in terms of the risk consequence and priority, highlighting the security measures that must be implemented; and,
 - ii. Illustrate the reduction of risk achieved in each case by updating the risk levels contained within the risk assessment, should the recommended measures be implemented.
- b. For structural elements that are concluded in the BEA report to be inadequately protected, and if the security solution requires structural hardening/enhancement, the CP shall prepare and submit the SRS report, supporting the CP's recommendations for structural hardening measures to mitigate relevant vulnerabilities and risks identified in the risk assessment with the analysis carried out in accordance with the requirements stipulated in [Annex D](#). The CP will design the structural elements based on validated approaches. SRS reports are not required for SDs or SIs that do not need structural hardening.
- c. The security measures proposed by the CP must comply with prevailing statutory requirements, codes or guidelines published by government authorities. This includes, but is not limited to, URA's development control parameters, BCA's Building Code, SCDF's Fire Safety Code, and/or other relevant international codes such as the International Ship and Port Facility Security (ISPS) Code.
- d. The CP will have to work with the RP's appointed representatives and Qualified Persons (**QPs**) to incorporate the final security measures into relevant project plans.
- e. Should certain security specifications or designs require amendments, the CP will carry out the necessary amendments, incorporate the necessary revisions to the original analysis to all relevant reports and submit the revised reports for the RP's approval.
- f. The RP must then select the final set of protection measures, after making the trade-offs between security and other considerations, such as cost, operational effectiveness and aesthetics. This involves determining and acknowledging the level of risk (i.e., residual risk) which remains after measures have been put in place. This should be done in consultation with CPS.
- g. The decision by the RP on the final set of protection measures and acceptance of residual risks⁵ (and associated responsibility) must be deliberated and endorsed in writing by a sufficiently senior representative (e.g., Emergency Planning Officer (**EPO**) or Chief Executive). This is to be done in consultation with the Sector Lead Agency.
- h. The SPP report should also include all the necessary details for the implementation of the security measures, including security design features

⁵ Residual risk is defined as the risk that could not be fully mitigated despite putting in all measures and controls.

that had been developed from the TVRA, BEA and SRS, and all necessary certifications, test data, calculations and drawings relevant to the Facility. A Summary Table of the Mitigation Measures (**SMM**) to be implemented is to be included in the SPP report submitted. The SMM should include a schedule specifying the implementation schedule for security measures, covering:

- i. Security measures that are required to be implemented before or upon the completion of specified works; and,
 - ii. Security measures that are required to be implemented after the Commissioner's approval of the Certificate of Works Completion (CWC), following the completion of specified works.
- i. For detailed requirements for SPP report, please refer to [Annex E](#).
 - j. The SRS and SPP reports can be submitted concurrently to CPS. Thereat, additional comments will be provided, if any, to the RP. The RP and CP have to address these comments and propose amendments, if required. The review may be carried out over a few iterations and the RP has to go through the CP's reports, clarifications and agree on the protective measures to be adopted.
 - k. Finally, the CP is to update the reports with the necessary amendments, clarifications and supporting information after the reports have been accepted.

Shelter Report (for Purpose-built Shelter, if applicable)

- a. Shelter Report needs to be submitted for CPIs equipped with Purpose-built Shelters. The CP shall recommend a comprehensive suite of protection measures to achieve shelter protection and the RP's security objectives.
- b. In the development of Purpose-built Shelter design, the CP shall prepare and submit the Shelter Report to ensure the safety and security of the occupants. The Shelter Report shall be submitted for review during the review of TVRA and SPP reports. Please refer to [Annex J](#) for more details.
- c. The CP shall ensure that the design principles and parameters for the shelter components are included in the Shelter Report.

How to minimise delays to the SBD process?

To minimise delays, RPs can: -

- Engage a security and/or blast consultant early to work with the project architects and engineers to incorporate security considerations upstream in the design;
- Proactively manage the security and/or blast consultants and vet the security reports carefully before sending them to CPS for review;
- Provide clear guidance to the security and/or blast consultants on key decisions such as critical assets and security measures to be adopted;
- Avoid major changes to the building design midway through the security review;
- Take an active role to ensure that the CP addresses queries raised by CPS in a timely and complete manner; and,
- Adopt the templates for the reports provided by CPS and the requisite analysis method.

Step 5: Application for Approval of Security Plan

74. When CPS has no further comments to the TVRA, BEA, SRS and SPP reports (collectively termed as "Security Plan") for the SD/SI, the RP can proceed to submit the application for Approval of Security Plan found on our [website](#). The application must be accompanied with the finalised Security Plan and such other documents that may be required by the Commissioner.

75. Upon approval, the Security Plan will be termed as the approved Security Plan (**ASP**). The RP can only start the specified works after obtaining the ASP.

Application for Commissioner's Approval of Amendment of Approved Security Plan before the completion of specified works

76. The RP or the Commissioner may at any point in time request for amendments to the ASP. Depending on the scope of the amendments, revisions to the TVRA, BEA, SRS and SPP reports may be necessary. Once the Commissioner approves the amended Security Plan, it will supersede the previously approved Security Plan and be recognised as the ASP.

Supervise implementation of security measures during specified works

77. The CP is required to oversee the specified works (whether construction or major renovation) to ensure that all the security measures are implemented as spelt out within the ASP. This includes overseeing the supply, deployment, construction, installation, testing and commissioning of the security measures/systems, and ensuring that these measures/systems are implemented according to the technical specifications and standards spelt out in the ASP.

Documentation

78. The CP must verify that the method statements, shop drawings, materials and workmanship specifications submitted by the vendor/contractor are in accordance with the specifications of the construction tender as awarded which includes the requirements of the ASP. If the contractor proposes any deviation from the security measures as spelt out within the ASP, the CP shall advise the RP whether the deviation is acceptable. Please refer to [Annex F](#) for the submission requirements for the construction phase.

Assess changes to Approved Security Plan (if any)

79. The RP shall update CPS if there are deviations from the ASP, due to issues such as unforeseen site issues or operational constraints during construction. The RP has to ensure that these changes will not lead to a lower level of protection for the critical processes and assets specified in the ASP. CPS will determine whether there is a need to re-assess the new security risks and to seek Commissioner of Infrastructure Protection's approval to amend the ASP accordingly. Please see [Annex G](#) for list of amendments that do not require approvals.

Application for Commissioner's Approval of Certificate of Works Completion

80. Upon the completion of specified works, the RP is required to submit the application for approval of CWC with the supporting documents to show that measures have been implemented in accordance with the ASP. Please refer to [Annex H](#) on the requirements for application for approval of CWC. For security measures that will be implemented only after the Commissioner's approval of the CWC (e.g., security manpower deployment), the RP should provide an indicative implementation date in the CWC. The RP should ensure that there are no deviation from the ASP.

81. The issuance of approval for CWC will only be considered after a site inspection and the proper submission of documents and clearances. After the requirements for approval of CWC have been fulfilled, CPS will take about 20 working days to process the application.

Audits and Enforcement

82. SDs/SIs may be randomly selected by CPS to be audited to ensure that security measures stated in the ASP and approved CWC are implemented and maintained to be in good working condition.

83. If there is any deviation from the ASP or approved CWC, the Commissioner may direct the RP in writing to take the necessary steps to rectify such deviations.

List of Abbreviations and Annexes

A&A	Addition and Alteration
ACMV	Air Conditioning and Mechanical Ventilation
BCA	Building and Construction Authority
BEA	Blast Effect Analysis
CBR	Chemical and Biological and Radiological
CPI	Critical Physical Infrastructure
COLPRO	Collective Protection
CP	Competent Person under the Infrastructure Protection Act
CPS	Centre for Protective Security, Ministry of Home Affairs
CSC	Certificate of Statutory Completion (from BCA)
CWC	Certificate of Works Completion
EPO	Emergency Planning Officer
EPV	Explosion Protection Valves
FE	Forced Entry
GEBS	Guidelines for Enhancing Building Security in Singapore
IPA	Infrastructure Protection Act
MHA	Ministry of Home Affairs
M&E	Mechanical and Electrical
NE	National Emergency
OBV	Overpressure explosion Protection Valve
OV	Overpressure Valve
QP	Qualified Person
RP	Responsible Person under the Infrastructure Protection Act
SBD	Security-by-Design
SCDF	Singapore Civil Defence Force
SD	Special Development
SI	Special Infrastructure
SOP	Standard Operating Procedure
SPP	Security Protection Plan
SRS	Structural Resiliency Study
T&C	Testing and Commissioning

TOP Temporary Occupation Permit (from BCA)
TVRA Threats, Vulnerability and Risk Assessment
URA Urban Redevelopment Authority



COMPETENT PERSON (SECURITY/BLAST)

- 1 Responsible Person's (RP's) Duties
 - 1.1 Under Section 33 (1) of the Infrastructure Protection Act 2017 (IPA), any security plan (including any amendment to the security plan) required or submitted to the Commissioner in connection with any specified works for a Special Development (SD) or Special Infrastructure (SI):
 - a. must be prepared by a person approved by the Commissioner in connection with those specified works (the Competent Person (CP));
 - b. must be prepared in such form and manner as the Commissioner may require; and
 - c. must contain the CP's security risk assessment and the security measures required for that SD or SI.
 - 1.2 Under Section 39(3) and 46(3) of the IPA, the Certificate of Works Completion (CWC):
 - a. must be prepared by a person approved by the Commissioner to prepare that certificate of works completion (the CP);
 - b. must be in such form and manner as the Commissioner may require; and
 - c. must contain the CP's certification that the security measures mentioned in section 38(1)(a) have been implemented in accordance with the approved security plan (ASP)
 - 1.3 The RP shall engage a CP (Security) and a CP (Blast) to comply to the above. The CPs will provide the RP with the SBD requirements which includes time management, security risk assessment, recommendations and certification of the implemented security measures.
 - 1.4 The RP shall however be ultimately responsible for the decision and outcome of the SBD review for the SD/SI. Please see [Annex A1](#) for a guide on how RPs should work with CPs to manage SBD projects.
- 2 Assessment Criteria for CP
 - 2.1 Relevant experiences (in recent three years) in the preparation of Security Plan under the MHA Security-By-Design (SBD) Process;
 - 2.2 Professional association and affiliations; and/or
 - 2.3 *[Depending on the nature of Project]* Relevant subject matter expertise and knowledge, with accredited referee reports or internationally published professional work.

3 Application Process

3.1 The application process to follow and comply are as detailed below.

Item	Details required when Responsible Person submits for the Approval of Competent Person (Security/Blast)
a	G50 form for security screening.
b	<i>[If name is not on whitelist as of date of application]</i> Please provide a detailed (i) Declarations of education, qualifications, skills and experiences; and (ii) Declarations of credentials and subject matter knowledge with referee reports and internationally published professional work, if applicable.
c	Curriculum Vitae (max. 1 page of self-description)
d	Application Form for Approval of Competent Person
e	Any other supporting documents

4 Change of Competent Person

4.1 If any approved CP becomes unwilling or unable to act, whether by reason of the termination of his appointment or for any other reason, to carry out his respective duties, the Responsible Person shall —

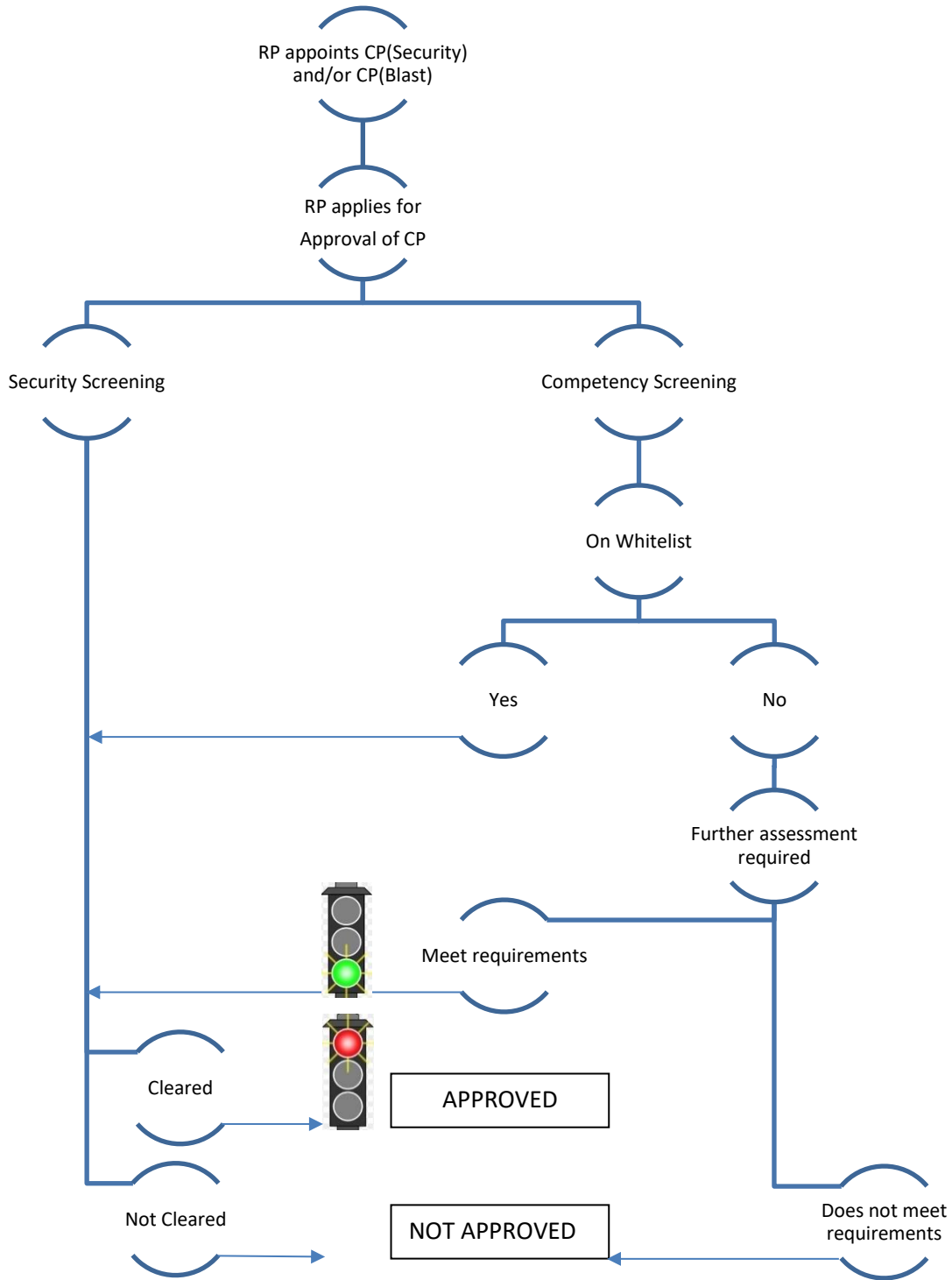
- a. Without delay appoint another CP in his place; and,
- b. Submit the Incoming CP for the Commissioner's approval.

The process to follow and comply are as detailed below.

Status	Procedures	Remarks
Change of CP before approval of Security Plan	RP shall notify Commissioner of Infrastructure Protection of the change by submitting Notice of Termination/ Replacement of Competent Person for Approval.	Outgoing CP shall have no objections for the incoming CP to use/adopt/develop on his current works to carry on with the preparation of the Security Plan.
Change of CP after approval of Security Plan but before approval of CWC		Outgoing CP shall still be responsible for the ASP. However, he shall have no objections to the right to use of the ASP he prepared. Any future amendments to the ASP shall be under the responsibility of the Incoming CP unless there is further change of CP. Incoming CP shall be responsible for the implementation of security measures and apply for the approval of CWC. He has the duty and accountability to keep records of the security measures supervised by the Outgoing CP. To avoid dispute, an agreed cut-off date shall be established.
Change of CP after approval of CWC		Under Section 40(2b) and 47(2b) of the Infrastructure Protection Act 2017 (IPA), the RP is responsible to maintain every security measure that is implemented in accordance with the ASP. If there is no security measure to be implemented after the approval of CWC, the RP shall be responsible to maintain the security measures implemented.

If there is security measure to be implemented after the approval of CWC, Incoming CP shall be responsible for the implementation in accordance with the period specified in the ASP.

5 Process Flowchart



1. Introduction

- 1.1. This section provides practical pointers on how RPs can work effectively with CPs to manage SBD projects. While CPs possess technical knowledge, SBD projects are relatively uncommon and can involve unfamiliar concepts for RPs. These pointers aim to help RPs maintain oversight of the project, ask the right questions, and make informed decisions throughout the project. They also reinforce the importance of clear roles, mutual accountability and being alert about potential gaps or overreach in technical recommendations.
- 1.2. The pointers are organised into three sections, highlighting what RPs should watch out for, ask, or act on to ensure that Security and Blast (S&B) requirements are properly integrated and managed through the CPs.

2. Pre-SBD review phase (up to Kick-off Meeting)

- 2.1. The objective in this phase is to lay the groundwork for security planning and ensure that early project activities align with future SBD requirements. Key points for RPs to note are:
 - a. Involve security consultants/advisors early: It is a good practice to involve security consultants/advisors during concept development as their early inputs can help to design the building with security in mind. However, it is important to note that they might not have been appointed as CPs under the IPA.
 - b. Control information security: Ensure that early participants (consultants, vendors, etc.) are security-screened where necessary, especially if sensitive layouts or threat assumptions are discussed. Access to project information must be limited to a need-to-know basis.
 - c. Engage Sector Lead or Ministry for advice: RPs should tap on experience from Sector Leads as this can provide clarity on typical SBD expectations and avoid rework later.
 - d. Define security objectives clearly: Work with consultants to identify critical assets, access requirements and potential threats. Document these in the project brief or concept design to ensure continuity when CPs are appointed.
 - e. Start planning for engagement of CPs: Identify potential CPs early and plan procurement timelines to avoid delays at the review phase. RPs should be clear about the deliverables and scope of work of CPs, which normally would cover the entire project lifecycle.
 - f. Start preparation for Kick-off Meeting (KOM): RPs must come prepared with the security objectives, project timeline and relevant site information, as well as any internal policy decision that may impact the security design e.g., deliberate choice not to undertake structural hardening due to operational disruption risks or other trade off.

3. SBD Review Phase (KOM to Approval of Security Plan, before Construction)

3.1. The objective in this phase is to work closely with the CPs to ensure that all S&B requirements are integrated into the design, properly documented in the Approved Security Plan (ASP), and coordinated across disciplines before construction begins. Key Points for RPs to note are:

- a. Ensure formal appointment of CPs: RPs must seek Commissioner of Infrastructure Protection's approval to appoint the CPs.
- b. Track Progress Closely: CPs report directly to the RP for all security-related matters. RPs should clear all SBD reports and be kept in the loop for all correspondences with CPS. RPs should also ensure adherence to project timeline. When delays are anticipated, RPs should take the initiative to notify CPS and request for more time, if required.
- c. Cross-Check assumption early: RPs should be clear and understand the key assumptions used by the CPs when managing the SBD project e.g., assumed threat types, standoff distances, and the definition of critical assets. RPs should also validate to ensure that these assumptions match the operational needs and project constraints.
- d. Ensure integration across design disciplines: RPs should ensure that security design measures are incorporated into architectural, structural, and M&E plans. They should lead coordination efforts to ensure no gaps, overlaps or scope mismatches. If the CPs are hired separately from the main project team, RPs should ensure that the CPs receive the support they need to develop the security plan.
- e. Review draft reports thoroughly: RPs should set internal checkpoints to review the SBD reports before their submission to CPS. When considering the solutions proposed to mitigate the residual risks, RPs should ask the CPs whether the solutions are practical, maintainable, and proportionate to the threat. If unsure, RPs should seek CPS inputs before signing off.
- f. Maintain a change log for design adjustments: Changes to the building design may affect the risk profile and require a revalidation of the SBD reports. If design change occurs (e.g., increase in number of floors, basement redesign, etc.), RPs must track these changes and alert the CPs immediately.

4. Construction to Certification of Works Completion phase (CWC to TOP)

4.1. The objective of this phase is to ensure that security measures stated in the ASP are faithfully implemented during construction, in order to obtain CWC, a prerequisite for TOP. Key Points for RPs to note are:

- a. Keep the CPs involved throughout construction: The CPs should stay engaged from start to finish as their roles do not end with the approval of Security Plan. RPs should ensure that the CPs are given access to construction meetings and site inspections to verify S&B related works follow the ASP.
- b. Manage design or site changes proactively: RPs should flag up any variations that affects the approved security measures to the CPs for assessment. If the changes are significant, an amendment to the ASP may be required.

- c. Guard against time or cost driven shortcuts: RPs should be aware of situations where contractors may propose substitutes or shortcuts for S&B measures due to budget or schedule pressure. RPs must ensure that the CPs are consulted before accepting any deviation.
- d. Track completion against ASP commitments: As works near completion, RPs should coordinate with the CPs to confirm all security measures stated in the ASP are in place and functional. A good practice is to request for period reports or photo documentation from the CPs to track the progress. RPs should not assume that all works are completed based solely on the reporting by contractor.
- e. Coordinate for CWC: The CPs are responsible to certify that all S&B measures have been implemented according to the ASP. Six months prior to the application for approval of CWC, CPS will arrange for a CWC KOM. RPs must ensure that the CPs complete the necessary documentation and sign off in a timely matter to avoid delays in the TOP process.
- f. Maintain a record for post completion review: RPs should keep a clear audit trail of CPs' submissions to RP, inspection notes, change logs and correspondences. These records will support future security reviews, audits or incident investigations.
- g. RPs play a critical oversight role throughout the project. By maintaining an active involvement and informed decision-making at each phase of the SBD review, RPs ensure that S&B requirements are properly designed and implemented.

KEY BUILDING DESIGN CONSIDERATIONS

1 Introduction

- 1.1 The concept design as well as the detailed planning and design stages of a building's development are key milestones to incorporate security considerations into the architectural layout, the structural design as well as the mechanical and electrical systems of the building. During the concept design stage, key issues to be considered include, but not limited to, site selection, building type, dimensions, positioning and orientation within the lot, landscaping as well as parking and vehicle flow. At the design and planning stage, important deliberations include, but not limited to, the structural scheme, characteristics of the envelop walls and facades, location of car parks and access roads, crowd flow, locations of critical assets and mass congregation areas.
- 1.2 Incorporating physical security concepts into the initial architectural design of a project is the most efficient and cost-effective way to achieve the required security level. Apart from the financial benefits of early planning for protection of the building, by considering the security aspects from the onset, early planning also allows architects and planners to work with security consultants to blend the required protection elements into the design of the building to achieve both security and aesthetic requirements. Information on the design considerations can be found in Guidelines for Enhancing Building Security in Singapore (**GEBS**). The following sections illustrate general design, structural and system issues which should be considered.

2 General Architectural Considerations

- 2.1 Security considerations should be deliberated during the initial stages of a development project such that cost effective protective solutions could be incorporated into the structural, layout and system designs, thereby reducing the need for hardening measures. Security measures can be integrated into the overall architectural design concept of the development in a seamless and unobtrusive manner. They can be designed in a manner such that they do not impede pedestrian movement and negatively impact the enjoyment of public spaces within the development.
- 2.2 Creating Stand-off Distance
 - 2.2.1 Stand-off distance is defined as the distance between the detonation point and the target building. Stand-off distance is the single most important factor when considering mitigation against the effects of an explosive attack. By increasing the stand-off distance, the resultant blast loads would be reduced, therefore saving significant effort and capital costs that would otherwise be needed to deal with the attack consequences. Therefore, the distance between a building and any road (or drop-off point, car park or loading/unloading bay with vehicular access) should be maximised, where feasible.
 - 2.2.2 However, given the scarcity of land in Singapore and the need to optimise land, large stand-off distance may not be feasible. Nevertheless, if adequate stand-off distance cannot be achieved, critical assets should be located away from the facade and towards the centre of the building.
- 2.3 Building Orientation

- 2.3.1 The orientation of the building may influence its risk against threats. For example, by taking advantage of the horizontal and vertical angles and obscuring the lines of sight from a potential threat, the risk against related threats may be reduced significantly.
- 2.4 Vehicle Anti-Ram Perimeter Line
- 2.4.1 The perimeter line should prevent unauthorised entry or the ingress of hostile vehicles through the use of crash rated fencing, barriers and bollards, etc. Anti-ram perimeter lines can be integrated into the overall architectural design concept of the building or within the design of the public spaces at grade with the road level. For example, where necessary, instead of crash-rated bollards, these structures can be integrated as part of the landscape features or streetscape infrastructure, such as public seating and planters.
- 2.4.2 Anti-ram measures shall be deployed in a comprehensive and consistent manner around the entire perimeter to mitigate hostile vehicle attacks. The penetration distance of the proposed crash-rated vehicle barriers should also be considered when determining standoff distances to critical assets.
- 2.5 Traffic Flow, Access Roads and Parking
- 2.5.1 Traffic is a challenging issue when planning a new building as vehicle access control and screening measures must be carefully planned such that it does not excessively impede the movements of vehicles into/in the premises. A smooth flow of traffic allows the security officers manning checkpoints to focus on their checks and not get distracted by the congestion. The flow of traffic must also complement, and not compromise, security of the premises.
- 2.5.2 As part of the Traffic Impact Assessment required for the development, additional security requirements could be considered and incorporated as part of the overall design for the building. For example, this should take into account the vehicle screening requirements such as the number of screening bays, the type of screening measures and the average time taken to screen each vehicle.
- 2.5.3 At an early stage, efforts should be taken to balance vehicle access control and screening requirements with having an efficient flow of traffic and people. Once the building has been constructed, it is extremely difficult to change the design and allocate space for such requirements. Hence, making sure that physical measures at access points are weaved into the overall traffic management of the premises (i.e., covering access roads, driveway, drop-off points, entrances to the building, and parking areas), will ensure proper functionality when the site is operational.
- 2.6 Mass Congregation and Critical Assets
- 2.6.1 Some areas in a building are characterised by the presence of large crowds. These areas of mass congregation are considered highly attractive for terrorists and therefore should be given special consideration during the design stage. Areas of mass congregation should be housed away from glass facades, main entrances or lower levels, where there could be direct impact from possible threats.
- 2.6.2 Critical assets (e.g., Security Control Room, Operations Command Centre, Building Maintenance Room, Fire Control Room, Data Centre, Server Room, etc.) or essential personnel, should also be housed at the core of the building or in specially protected areas, away from the threats i.e., away from publicly accessible locations.
- 2.7 Materials and Façade Systems
- 2.7.1 The choice of building materials has a direct impact to the physical integrity of the building. Each type of material offers a different level of protection due to its differing

hazard levels, for instance, cast in-situ reinforced concrete usually offer the best protection, whilst glass is inherently weak against blast. Special consideration must be taken when choosing the type of building materials, especially for the façade.

3 General Structural Considerations

3.1 Any type of building collapse must be avoided, but the most critical category to be avoided is progressive collapse. Past incidents have demonstrated that progressive collapse results in very high fatality rates and will cause significant collateral damage to humans, buildings and other structures in the surrounding area. To mitigate progressive collapse, protective measures should be directed towards strengthening primary structural elements.

3.2 Progressive Collapse Mitigation

3.2.1 Progressive collapse is defined as the spread of an initial local failure from element to element, eventually resulting in the collapse of an entire structure or a disproportionately large part of it. Progressive collapse occurs in most cases, due to the loss of one or more critical column supporting the building.

3.2.2 The primary structural elements are the essential parts of the building, which support the building and provide the resilience against progressive collapse in the event of a blast.

3.2.3 Typically, adopting a straightforward approach which involves designing primary structural elements against local failure for the given threat and stand-off distance would suffice.

3.3 Capacity for Resisting Shear Failure

3.3.1 It is essential that the primary structural elements maintain sufficient strength and ductility when undergoing flexural response to preclude a shear failure. When the shear capacity is reached before the flexural capacity, the possibility of a sudden, non-ductile failure of the element exists, potentially leading to a progressive collapse of the structure.

3.4 Multi-Storey and Underground Car Parks

3.4.1 During an explosion in an underground car park or enclosed area, the forces acting on the structure are different from those in an open location. Hence, it is essential to study the integrity of the structural system of the underground car park during the design and planning stage.

3.4.2 A blast in an underground car park is subjected to many reflections, where the impulse it creates is much higher compared to an explosion in the open. The lifting forces are therefore expected to be very high and a breach of floors and ceilings must be considered and studied. It is recommended that underground car parks are segregated into public and private car parks, with the public car parks placed outside the main building's footprint to prevent progressive collapse from unscreened Vehicle Borne Improvised Explosive Devices.

3.5 Blast Resistance

3.5.1 The ability of the structure or façade to resist blast pressure is a function of (i) the material composition of the structure and (ii) the section properties of the main structural elements, including the structural spans and the connection details. Selection of suitable resilient structural designs should be considered during the initial structural design phase to minimise the impact on the building's final design.

3.5.2 During the design and planning stage, a simple structural scheme consisting of a beam/column system should be adopted. Arising from the studies of the Oklahoma City attack, it is recommended that the use of large transfer beams should be avoided at public areas that are accessible by vehicles.

3.6 Workplace Shelters

3.6.1 Workplace Shelters are different from Purpose-built Shelters. Workplace Shelters are to be provided for Critical Physical Infrastructures which require essential personnel to be stationed in-situ to ensure the continued delivery of essential services.

3.6.2 The Workplace Shelter shall comprise of hardened spaces where the essential personnel could seek temporary refuge from the weapon effects. Generally, Workplace Shelters are co-located within a critical asset room and sited at a location that is near where the essential personnel are expected to be stationed.

3.7 Forced Entry Resistance

3.7.1 Forced entry (**FE**) is a tactic commonly used to penetrate critical areas through the use of hand or power tools. While the critical asset room could be secured with electromagnetic locks and monitored using intrusion detection devices, vulnerable areas could be exploited for unauthorised entry e.g., unsecured doors and windows, utility portals and ventilation shafts.

3.7.2 A good understanding of the structural components and locking mechanisms enables building designer to select FE resistant components such as reinforced concrete walls, FE resistant doors, etc.

4 Mechanical and Electrical System Considerations

4.1 The general design and security considerations for mechanical and electrical systems, including that of backup generators, should be considered at an early stage. For the design of switchrooms and relevant electrical connections, please refer to SP Group's "How to Apply for Electricity Connection" handbook (<https://www.spgroup.com.sg/home>). Compatibility and integration with the general design in the initial stage will help achieve an effective assimilation of systems into the overall building. Such considerations will also prevent conflict between the system requirements and other factors such as the urban planning, landscaping, lighting and fire safety.

4.2 The solutions should take into consideration the capacity for future upgrades, expansion and replacements. Any software and hardware used should therefore be modular and upgradeable with adequate physical space catered for future replacement.

4.3 Typically, many systems are either shared by security, safety and administration or take into account the requirements and environment of each other. This must be considered at an early stage to ensure that the requirements of all parties are met and that there is adequate integration between them.

4.4 Power Supply

4.4.1 As a practice, providing redundancies and backups to the power supply should be adopted. Firstly, multiple feeds from the public utility should be provided to enhance diversity and ensure no single point of failure. Secondly, an Uninterruptible Power Supply (UPS) to provide a minimum period of backup power should be installed to ensure continuity of services at the initial stage. Thirdly, provision of on-site standby diesel

generators to sustain power for longer term outages. The electrical power system should be designed to support continuity of vital functions in the aftermath of an attack i.e., a smooth cut over to emergency electrical power supply.

- 4.4.2 The UPS and backup diesel generators are crucial in maintaining a constant flow of power in the event of a power failure from the public utility. The UPS should be adequately sized to support the power demand of all vital functions e.g., all computer and data centre equipment, mechanical and ventilation systems, fire safety systems and electrical devices (such as emergency lighting and security equipment), minimally for the time taken to switch over to the emergency power supply or the standby generators. In addition, it must take into consideration the "peak" load or fault overload conditions i.e., the surge in power demand when the equipment is first energized. As a rule of thumb, the UPS should be sized for 150 percent of the operating demand and be continuously operational to filter and condition the power supply.
- 4.4.3 Diesel generators should be provided to generate power for longer term outages, if the UPS is not suitable for long term provision of emergency power supply. The generators should be maintained and tested periodically to ensure their operational integrity. Sufficient fuel supply should also be catered to sustain the generators for the outage duration.

REQUIREMENTS FOR THREAT, VULNERABILITY AND RISK ASSESSMENT (TVRA)

1 Introduction

- 1.1 The TVRA is a systematic process to identify and analyse risks associated with attacks against the identified critical assets of an infrastructure. Although numerous methodologies have been developed, the principles of conducting risk assessments are generally similar in nature. The objective is to provide a prioritised list of risks to facilitate the Responsible Person's (**RP's**) decision on the mitigation measures to be adopted.

2 Key Elements

- 2.1 In conducting TVRA, the following key elements are generally considered:
- a. Introduction of the infrastructure and its critical function;
 - b. Security objective of the review and TVRA methodology;
 - c. Identification of critical assets;
 - d. Definition of threat scenarios;
 - e. Assessment of threat probability;
 - f. Analysis of vulnerability;
 - g. Analysis of consequences/Impact of successful attack;
 - h. Evaluation of risk; and,
 - i. Explanation of implications of risk assessment/conclusion.
- 2.2 The TVRA is an iterative process where the RP needs to work closely with the Competent Person (**CP**) to agree on the risk assessments. The RP will endorse the final report and submit it to the Centre for Protective Security (**CPS**) for review.
- 2.3 The TVRA report should comprise the key items mentioned in paragraph 2.1 in separate chapters and should generally follow the order mentioned.

3 Introduction of the infrastructure and its critical function

- 3.1 The introduction should include the location of the infrastructure, the external surrounding area and the internal layout including the general operations/business function of the premise. General details such as timing and flow of persons, vehicles, goods, etc. should also be included. The introduction should also describe the concept of operation of the infrastructure, the critical function that it performs and, if necessary, the need for a Workplace Shelter or Purpose-built Shelter.

4 Security objective of the review and TVRA Methodology

- 4.1 The security objective serves as a foundational statement that defines the intended security outcomes of the Critical Physical Infrastructure/High Profile Development. It aligns security measures, risk mitigation strategies, and compliance requirements to ensure that resilience and protection of the facility against threats. The security objective of CPIs should be supported by the Sector Leads (SLs).

- 4.2 There is no preference for any particular TVRA methodology, as long as it is relevant to the nature of the assessment to be done and the CP is able to clearly demonstrate ability and experience in applying the methodology. As a general guide, the methodology employed should be able to express the risks faced by the assets in terms of the threat considerations, the impact of a successful attack, the relative importance of the defined assets, the attractiveness of the premises as a target, and any site-specific weaknesses that may be exploited. The methodology should also allow for the clear and concise presentation and prioritisation of risks. A description of the TVRA methodology adopted including the assumptions made should be documented.
- 4.3 The risk analysis **SHALL NOT** merely be a building-level analysis. Instead, various types of plausible threat scenarios⁶ within the infrastructure shall be developed and assessed. For each threat scenario, a robust and soundly supported assessment of the risks faced by the individual critical assets, using the proposed methodology, shall be made. In assessing each threat scenario, consideration should be taken for the typical security features found in the type of infrastructure being studied or features that have been incorporated in the infrastructure's design⁷. For threat scenarios involving Improvised Explosives Devices (**IEDs**) and explosive weapons, analysis should be supported with the relevant facts, figures, quantitative and qualitative data as derived from calculations, computer simulations, actual tests, literature review, etc. to assess the risk of each scenario.

5 Identification of Critical Assets

- 5.1 The first step of a proper TVRA is to identify the critical assets within the infrastructure. These critical assets will then become the focus for the rest of the assessment process.
- 5.2 Critical assets are generally defined as assets which are vital for the infrastructure to perform its function. When identifying critical assets, the RP needs to consider what are the critical functions/services that the infrastructure provides as well as the infrastructure and equipment required to support these functions/services. Critical assets should be defined in consultation with stakeholders.
- 5.3 For large buildings with high public footfall, the focus would be in preventing mass casualties in areas of mass congregation.
- 5.4 For critical asset identification, the following should be addressed:
- Are there any interdependencies among the assets?
 - What are the existing countermeasures?
 - What are the consequences if the asset is damaged?⁸
 - Are there any effective redundancies⁹ available; and,
 - Where are the assets located?¹⁰
- 5.5 If a Workplace Shelter is required, it can be co-located in the same space with a critical asset.

⁶ This represent threat scenarios at the various locations within the infrastructure where the critical assets may be at risk. For example, a vehicle borne IED (VBIED) at the vehicle drop-off point, a chemical and biological attack using the ventilation system at a particular air intake point, etc.

⁷ For example, the CP should take into account the envisaged operational flow of the infrastructure i.e., whether it is open for public access, whether screening will be conducted on vehicles or persons entering, whether security clearance will be conducted for personnel working in the building, etc.

⁸ This should include expected downtime if the asset is damaged and whether it can be restored.

⁹ To assess the effectiveness of these redundancies, CP should check whether these redundancies will be damaged together with the assets by a single threat scenario.

¹⁰ The location of the assets should be clearly indicated on a layout plan.

- 5.6 Given that the identification of critical assets is such a crucial step, the RP may wish to seek comments from CPS and their SL before the CP proceed with the analysis for the TVRA to avoid abortive work.

6 Definition of Threat Scenarios

- 6.1 The baseline threat list is controlled and disseminated to the RP¹¹.
- 6.2 Where applicable, the CP should include cases of previous attacks conducted on similar facilities within the report.
- 6.3 The CP is also expected to study and include threats which are not within the threat list but are specific to the infrastructure being assessed.
- 6.4 To conduct proper threat scenario identification, the CP should address the following:
- Have all threats on the baseline threat list been considered? If not, are justifications provided for their omission?
 - Have the baseline securities been included?
 - Have the different methods of delivery been considered in the threat scenarios?

7 Assessment of Threat Probability

- 7.1 The probability/likelihood of terrorists attempting a threat is typically computed as a score. Different methodologies have a different scoring range (e.g., 1 to 5 or 1 to 10, etc.) with '1' normally being low and '5' or '10' being high. This must be conducted at the asset level where applicable.

8 Analysis of Vulnerability

- 8.1 Vulnerability analysis¹² estimates the likelihood that a terrorist/adversary will be successful in executing a specific attack mode on the infrastructure.
- 8.2 The CP shall consider the following factors:
- The asset's visibility (ease of obtaining building information in public domain or through reconnaissance);
 - Existing/baseline security measures and Standard Operating Procedures (SOPs) that can (or aid to) detect, delay, deny the threats; and,
 - Geographical/site disadvantage e.g., lack of standoff distance due to site constraint, etc.

9 Analysis of Consequence/Impact

- 9.1 Consequence analysis¹³ estimates the impact of a successful attack on the infrastructure. The CP shall minimally consider the following factors:

¹¹ RP should ensure that CP is security cleared before disseminating the threat list

¹² If there are varying levels of security for the infrastructure, different vulnerability assessments may be needed for different time periods.

¹³ If there are varying levels of consequences for the infrastructure, different consequence assessments may be needed for the different time periods e.g., whether building is hosting high-signature events for MICE venues.

- a. Loss of lives;
- b. Loss or damage to building/critical assets; and,
- c. Loss of primary service/output capability (downtime).

9.2 For blast effects, quantitative analysis should be used to determine the consequence/impact. This analysis, which is sometimes called the Blast Effects Analysis, may be contained in a separate annex to be submitted together with the main qualitative TVRA report. The CP can provide qualitative assessments in the TVRA report (and quantitative assessments with detailed calculations thereafter in the Structural Resiliency Study) if the conclusion is that additional mitigation is required.

10 Evaluation of Analysis

10.1 This phase of the assessment generally relates the ratings of threat with vulnerability and consequence to achieve a risk rating. The figure is then used for prioritising or ranking the risks to carry out risk management proposals or countermeasures. This is important to the RP as it helps them to make decisions on the risks that need to be addressed critically and the risks that can be managed with existing measures.

10.2 The analysis should contain a clear list of risk arising from the different threat scenarios against the individual CAs.

11 Implications of Risk Assessment/Conclusion

11.1 The broad implications of the analysis should be presented as a conclusion. This should include:

- a. A clear listing of risks which are deemed to be acceptably low enough for additional mitigation measures not to be taken; and,
- b. A clear list of risks to be mitigated and a broad description of the types of mitigation measures¹⁴ which would be undertaken, and/or further analysis which will be conducted to propose suitable mitigation measures.

12 TVRA Report

12.1 An outline of the TVRA Report can be found in Annex C1. This outline serves as a guide to illustrate what are the essential information to be included and how these information can be presented in a more systematic manner.

¹⁴ Examples include "full height steel jacketing for columns directly exposed to potential blasts in the atrium will be explored and its specifications elaborated upon in the SRS", and "laminated tempered glass in the auditorium will be explored and its specifications elaborated upon in the SRS".

1. The TVRA report details the process to identify and analyse risks associated with attacks against the identified critical assets of an infrastructure and provide a prioritised list of risks to facilitate the RP's decision on the mitigation measures to be adopted.
2. To facilitate the Security-by-Design review, the CP should ensure that the TVRA report has comprehensively covered the following key areas:
 - a. Executive summary
 - b. Introduction
 - i Background of the project
 - ii Classification of the development
 - iii Site characteristics
 - iv Location of the infrastructure
 - v Scope of TVRA
 - vi General information of the business, function, operation, Business Continuity Plan, alternate site, etc.
 - vii General information of the building operations/security/facility characteristics
 - viii Drawings
 - (a) Location map/site layout with illustration of the internal/external roads and adjacent buildings
 - (b) Building footprint including perimeter line, vehicular/staff/public/restricted accessible areas, staff/public carpark, loading & unloading accesses/bays, security control rooms, restricted areas within building, locations of critical assets, areas of mass congregation, etc.
 - (c) Cross section of the building
 - (d) Staircases/escalators/lifts/fire escape shaft/staircase

[Please provide clear markings and explanations for all drawings including, labeling, legend, layering, orientation, traffic/pedestrian ingress/egress, etc.]
 - c. Security objectives of TVRA
 - d. TVRA Methodology. Details of the TVRA methodology used in the report including definition of T, V, C and risk scores.
 - e. Identification of critical assets
 - i Table of critical assets
 - ii Critical asset details (see **Table1**)
 - iii Single line diagram
 - iv Location map of critical assets with label
 - f. Baseline Security Measures
 - i Description of the existing Security Measures by layers including operational, technological and physical measures
 - ii Location maps and photos of measures
 - iii Testing and Certification
 - iv Plans for additional security measures during contingency
 - g. Define Threat scenarios
 - i Design Based Threat
 - ii Details of threat scenarios
 - h. TVRA results

- i Risk Score Table (see **Table 2**)
- ii Determining area of high risk
- iii Prioritising or ranking of risks
- iv Interpretation of the TVRA results
- v Detailed TVRA calculation enclosed in Annex

- i. Conclusion

Table 1

S/N	Critical Asset	Quantity	Functions	Operational Impact	Redundancy/Contingency	Estimated Replacement Lead Time	Cost

Table 2

S/N	Critical Asset	Threat Scenarios	Risk Score (highest to lowest)	Ref no. to detailed calculation in ()
		xx threat at yy location	200	

REQUIREMENTS FOR BLAST EFFECT ANALYSIS (BEA)/STRUCTURAL RESILIENCY STUDY (SRS)

1. Introduction
 - 1.1 The BEA is conducted at a component level to establish the survivability of key components which are subjected to blast threats and the SRS identifies the vulnerabilities documented in the BEA and recommends mitigation measures to enhance the overall structure resilience against blast. This section describes the requirements of BEA and SRS for Critical Physical Infrastructures and High Profile Development.
2. The BEA/SRS reports shall include:
 - a. Derivation of the explosive loads:
 - i. blast overpressures (free-field, reflected and/or confined);
 - ii. fragmentation;
 - iii. explosion-resultant fireballs; and,
 - iv. ground shock.
 - b. Indication of physical dimensions and material properties of all structural components analysed (including reinforcement details for reinforced concrete components);
 - c. Computation of the ductile mode response (i.e., flexure, diagonal and direct shear) of the building components;
 - d. Computation of the brittle mode response (i.e., spalling, breaching and cratering) of the building components; and,
 - e. Assessment of the consequences of the explosive loads on the critical assets.
3. Structural details and material properties from the structural engineering team, rather than assumed ones, shall be used for the analysis.
4. For response analysis of structural components (i.e., load-bearing members e.g., columns, beams, slabs, walls, etc.), the below specified methodologies shall be applied:
 - a. Single-Degree-Of-Freedom (SDOF) or Multi-Degree-Of-Freedom (MDOF)¹⁵ for analysis of ductile mode response (flexural, diagonal and direct shear) when subjected to air blast from an explosive charge at a scaled standoff distance of $\geq 0.4 \text{ m/kg}^{1/3}$. When the scaled distance is less than $0.4 \text{ m/kg}^{1/3}$, verified and validated numerical models shall be used, and no other methodologies will be accepted;

¹⁵ MDOF (rather than SDOF) shall be used where it is not appropriate to analyse a structural component from another connected component independently of each other.

- b. Methods found in Unified Facilities Criteria (UFC) 3-340-02 for determination of whether a concrete component will spall or breach when subjected to a case/uncased explosive charge in contact/near-contact;
 - c. Numerical modelling and simulation, provided that information on the validation of the numerical model with results of actual full-scale blast tests conducted on equivalent structural components and scaled distances is made available to the Centre for Protective Security (**CPS**) upon request.
5. For response analysis of non-structural components (e.g., brick wall, glazing, doors, equipment, etc.), the following methodologies shall be applied:
 - a. Methodologies and guidelines defined in established codes and/or literature, provided that a complete copy of the codes/literature used is made available to CPS upon request and that relevant sections of the codes / literature used in the analysis are clearly pointed out; and/or
 - b. Numerical modelling and simulation, provided that information on the validation of the numerical model with results of actual full-scale blast tests conducted on equivalent structural components and scaled distances are made available to CPS upon request.
6. For global structural response using Alternate Load Path analysis where a structural column or load-bearing wall is assessed to fail due to explosive loads, the analytical procedures set out in UFC 4-023-03 shall be adopted. Considerations such as dynamic increase factors, load factors, joints resistance functions, pass/fail criteria for joint rotations, etc. must be incorporated.
7. Results from actual full-scale blast tests can be used for analysis, provided that the tests are conducted with equal or higher blast loads on test subjects similar to the analysed components and that full information of the tests are made available to CPS.
8. CPS reserves the right to request for additional information and clarification from the CP on the methodologies used in the analysis.
9. The BEA and SRS Outline Templates can be found in [Annex D1](#) and [Annex D2](#), respectively. These templates serve as a guide to illustrate what are the essential information to be included and how this information could be presented in a more systematic manner.

Annex D1 – Blast Effect Analysis Outline Template

1. The BEA report shall be a document that presents a concise and comprehensive coverage of the following pertinent areas:
 - a. The key assessment outcomes of the identified components (cross-referenced from TVRA) which are exposed to the threats followed by their corresponding impacts/consequences on the critical assets of the building.
 - b. Risk prioritization on these outcomes according to the acceptance criteria which is agreed with the relevant stakeholder(s).

2. To facilitate the Security-by-Design (**SBD**) review, the CP (Blast) should ensure that the BEA report comprehensively covered the following key areas:
 - a. Executive Summary

The executive summary shall provide a brief summary of the purpose of the BEA study and summarise the BEA outcomes, similar to [Table A](#).

Table A – Summary of BEA Outcomes

S/N	Location	Element Type/ID	Existing Dimension	Existing Structural Details ¹⁶	Charge Weight & Standoff ¹⁷	Predicted Impacts/Consequences ¹⁸
E.g. 1	Atrium	Column / 2A4	L800mm x W800mm Span: 4m	Conc Gr: 40 MPa Steel Gr: 460 MPa Main Rebar: 12T20 Shear Links: T10@200 Connection Details	250kg @ 1.5m	Column fails.
E.g. 2	Office Room	Glazing / 4G5	L200mm x W300mm	Conc Gr: 40 MPa Steel Gr: 460 MPa Main Rebar: 10T40 Shear Links: T10@150 Connection Details	250kg @ 8m	Glazing fails, resulting in debris that may cause injury or death to critical personnel sitting inside office.

¹⁶ The structural details shall include (but not limited to) material grades, reinforcement details, connection details, etc, where applicable.

¹⁷ Standoff distance is defined as the distance measured from the centre of charge to the structural surface of the critical asset facility.

¹⁸ The CP shall ensure that the predicted impacts/consequences are reflected consistently in the TVRA report.

b. Introduction

This section shall provide a brief description of the project background, scope of the assessment and the security objective(s). It shall also include, but not limited to, the following pertinent information so that the reader has an overview understanding of the project.

- i. Classification of the development e.g., Category I/II Infrastructure under the Critical Infrastructure Programme (CIP) Framework or High Profile Development (HPD);
- ii. Whether it is a new development or Addition and Alteration (A&A) works. For A&A works, state clearly the changes/modification, preferably illustrating them on drawings;
- iii. Description of the structural framing system and boundary condition of the element;
- iv. Description of the development's locality and provide clear orientation of the development (e.g., illustrating public and restricted access areas on drawings);
- v. List of critical assets and threat scenarios (include the rationale behind the creation of each threat scenarios); and,
- vi. The locations of critical assets with their respective standoff distances from the threat shall be clearly illustrated on the drawings.

c. Design Methodology

This section shall provide concise and comprehensive description of the design approach (quoting all relevant references, code of practices and standards that are being adopted for the design). It shall also include, but not limited to, the following areas:

- i. Clear listing of all assumptions with appropriate explanation (substantiated with relevant references, code of practices and standards, if applicable) on why such assumptions are adopted;
- ii. Derivation of explosive loading (all applicable weapon effects are to be considered e.g., blast overpressure, confinement effects, fragmentation, fireball and ground shock);
- iii. Description of methodology/software (e.g., CONWEP, Shock & Frang, Autodyn, ETABS, etc.) for the derivation of each type of loading/weapon effects and the component responses to the structures;
 - For SDOF, methodology to derive the uniform distributed load is to be included.
 - If numerical simulation software is used, explanation on verification & validation of the results is to be included. (*Note that only the approved verification and validation of the software can be used for the numerical simulation.*)
- iv. Stating the appropriate acceptance criteria e.g., Glazing: GSA 3A, Support rotation: $\leq 2^\circ$ (PDC - Protective Design Center), Human and Equipment survival criteria; and,
- v. The design methodology and acceptance criteria shall be discussed and agreed with the relevant stakeholder(s) and the stakeholder(s)' agreement

in acceptance of the criteria and/or undertaking of any form of residual risks shall be properly documented in this report.

d. Blast Effect Analysis

The blast effect analysis is done at component levels in identifying the survivability of the key components which are likely subjected to the blast threats. Thereafter, determine the corresponding consequences and impacts on the critical assets of the building.

The various design checks are to be done in accordance with relevant and prevailing codes and practices, reference and standards. As a guide, CP(Blast) could refer to the design checks tabulated in Table for reference.

3. Finite Element Analysis (FEA) shall be carried out should the threat scenario be determined as "close-in" with a scaled distance of $z \leq 0.4\text{m/kg}^{1/3}$. Only FEA tools that have undergone verification and validation and are approved by CPS can be used. CP (Blast) is required to provide a FEA report for the analysis and the content of the report shall include, but not limited to, the following:

- a. A brief description of all the models that have been modelled e.g., model size/dimension, charge weight, standoff, etc.
- b. Material models for concrete.
- c. Material models for steel.
- d. Material models for reinforcement.
- e. Material models for the charge and detonation products.
- f. Element formulation used for the concrete, steel, reinforcement, air, charge and detonation products (Eulerian, Lagrangian, SPG, etc.).
- g. Coupling between the concrete, steel, reinforcement, air, charge and detonation products, if any.
- h. Erosion criteria used, if any.
- i. Boundary effects (extent of boundary to ensure no blast overpressure reflection from boundaries back to the area of concern, locations of the fixed boundaries in x, y, and z axis and how are they done in the FEA program, etc.).
- j. Application of axial load to the structural element after the blast event.
- k. Mesh refinement analysis with a minimum of 3 different mesh sizes that are not close to each other (preferably a factor of at least 1.4 from one another as a rule of thumb) so that convergence could be observed. The results should be plotted against the various mesh sizes analysed to show that the results plateau to a certain figure.
- l. Relevant output results from the model e.g., stress contours and other calculations to show how the residual capacities are being determined.
- m. Tabulation of the residual capacities obtained from the various mesh sizes. The one with the lowest value should be adopted for comparison with the actual load take of the structural element. Illustration of how the actual load take of the structure is being computed should be provided.
- n. Assumptions adopted for the model, if any.
- o. Any other information that is deemed appropriate and necessary to provide a better clarity of the analysis work.

4. The report should comprise, but not limited to, the above key items in separate chapters and should follow the order listed.
5. Relevant documents and drawings shall be attached in the Appendix of the report for easy reference and a suggested list is shown in Table B.

Table B – List of information¹⁹ required in the Appendix

S/N	Description of Documents/Drawings
1	Site/Location Plan
2	Architectural Layouts and Elevations ²⁰
3	Architectural Details e.g., opening sizes of doors, louvers, windows, etc. ⁶
4	Structural Layouts and Elevations ⁶
5	Structural Details e.g., dimensions and reinforcement details for columns, beams and slabs ⁶
6	Layout(s) showing the location of critical assets and their respective standoff distances from the threat
7	Layout(s) showing the demarcated boundaries of public and restricted access areas
8	Drawing(s) showing all changes that are relevant to the SBD submission for the facility (applicable for A&A works and any SBD amendment submission)
9	References, Code of Practices and Standards, where applicable
10	For Structural Components: detailed calculations for all local and global checks
11	For Non-Structural Components (e.g. glazing, equipment, roller shutter, etc): detailed calculations that are relevant to justify its survivability
12	For Human Injury Prediction: detailed calculations that are relevant to justify its survivability
13	Analysis and results from design software
14	Summary of ground shock analysis results for all critical assets to be tabulated in <u>Table C</u> .

¹⁹ Provide only those documents/drawings (NOT the entirety) that are relevant to this study. Drawings shall be provided in PDF format, A3 size with details clearly annotated. Reports and/or other kind of information shall be provided in PDF format.

²⁰ If detailed information is not ready to be included in the drawings, CP is to provide key preliminary information (e.g., indication of floor levels, access points, beams/slabs/columns/walls dimensions and rebar details, etc.) that are essential for the review.

6. Ground shock analysis results for all critical assets shall be tabulated as shown in [Table C](#) below.

Table C – Summary of Ground Shock Analysis Results for BEA Report

CA	Summary of BEA Findings (Shock Analysis) ²¹ Vv, Vh, Av, Ah						Design parameters for shock protection	Critical Asset Survivability (Yes / No)	Remarks
	Threat 1	Threat 2	Threat 3	Threat 4	Threat 5	Threat 6			
CA 1	Vv = Vh = Av = Ah =	Vv = Vh = Av = Ah =	Vv = Vh = Av = Ah =	Vv = Vh = Av = Ah =	Vv = Vh = Av = Ah =	Vv = Vh = Av = Ah =	Vmax = Amax =		
CA 2	Vv = Vh = Av = Ah =	Vv = Vh = Av = Ah =	Vv = Vh = Av = Ah =	Vv = Vh = Av = Ah =	Vv = Vh = Av = Ah =	Vv = Vh = Av = Ah =	Vmax = Amax =		
CA 3	Vv = Vh = Av = Ah =	Vv = Vh = Av = Ah =	Vv = Vh = Av = Ah =	Vv = Vh = Av = Ah =	Vv = Vh = Av = Ah =	Vv = Vh = Av = Ah =	Vmax = Amax =		
CA 4	Vv = Vh = Av = Ah =	Vv = Vh = Av = Ah =	Vv = Vh = Av = Ah =	Vv = Vh = Av = Ah =	Vv = Vh = Av = Ah =	Vv = Vh = Av = Ah =	Vmax = Amax =		
CA ...	Vv = Vh = Av = Ah =	Vv = Vh = Av = Ah =	Vv = Vh = Av = Ah =	Vv = Vh = Av = Ah =	Vv = Vh = Av = Ah =	Vv = Vh = Av = Ah =	Vmax = Amax =		

CP(B) to verify that the above in-structure shock values are accurate and updated based on the latest BEA report. Subsequently, CP(B) shall update the SPP report to highlight the associated residual risks and mitigation measures against ISS (see [Annex E](#)).

²¹ Units of measurement for velocity (V) and acceleration (A) are mm/s and g respectively. All shock calculations shall be endorsed by Professional Engineer.

1. The SRS report shall be a self-contained document that presents a concise and comprehensive coverage of the following pertinent areas:
 - a. The key assessment outcomes from the TVRA and BEA reports, and the resulting stakeholder(s) decisions on which risks to address and/or accept.
 - b. The proposed mitigation measures to be carried out on site.

2. To facilitate the SBD review, the CP (Blast) should ensure that the SRS comprehensively covered the following key areas:
 - a. Executive Summary
 - i. The executive summary must be presented in a clear and unambiguous manner, so as to facilitate the SBD review process as well as subsequent tracking, checks and/or audits of approved works by CPS.
 - ii. It shall cover the following main areas:
 - Essential background²² underlying this SRS report.
 - Summary of identified components²³ for “Actual Implementation” of mitigation measures (refer [Table D](#) for typical listing).
 - Layout(s) indicating the locations of the identified components with respect to those of the critical assets.
 - Key assessment outcomes from TVRA and BEA, and the resulting stakeholder(s) decisions on which risks to address and/or accept.

Table D – Summary of identified Components for Implementation of Mitigation Measures

SN	Location	Layout ²⁴	Critical Asset		Component		Proposed Mitigation Measure	
			Name	Blast Effect	Type	ID	Description	Schematic ²⁵
1					C	1		Refer to Annex Page 1
2					C	2		Refer to Annex Page 1
3					B	1		Refer to Annex Page 2
4								
5								
6								
7								

²² Two main aspects; (i) key assessment outcomes from TVRA & BEA, and (ii) the resulting stakeholder(s) decisions on which risks to address and/or accept. As per standard international practices, protective security design is a risk-tiered process i.e., not all risks can be addressed within practical means, and hence focus ought to be accorded to scenarios of higher risks. CP (Blast) must assist stakeholder(s) to rationalize a practical way forward in view of other non-security operational requirements. For A&A projects, it is of utmost importance that existing site constraints are accounted for upfront during design.

²³ These involve both structural and non-structural components. Typical listing include column, wall, slab, beam, brick wall, door, window systems, etc. Component supports e.g., frame and mullion design for glazing, which are integral to the overall blast-resistant performance, must be accounted for.

²⁴ Layout(s) contain the locations of the identified components with respect to those of the critical assets. These part-prints in pdf must only include relevant dimensions and markups. Irrelevant layers in original drawings e.g., M&E services, architectural features, etc. must be omitted for ease of reference.

²⁵ The submitted schematics must indicate all relevant details, such as reinforcement arrangement for concrete components, glazing layup and frame bite, door stiffeners etc. to be done in accordance with prevailing standards such as ASCE 59-11, UFC 3-340-02, PDC TR-06-01, PDC TR-06-12, etc. They can be included as separate annexes for ease of reference. These contents must reflect buildable designs with actual site implementation in mind, for avoidance of doubts.

8								
9								
10								

Legend²⁶

C	: Column
W	: Wall
S	: Slab
B	: Beam
BW	: Brick wall
D	: Door
G	: Window Systems

b. Introduction

This is similar to the "Introduction" in the BEA Report Template.

c. Design Methodology

This is similar to the "Design Methodology" in the BEA Report Template.

d. Protective Hardening Measures Design Analysis

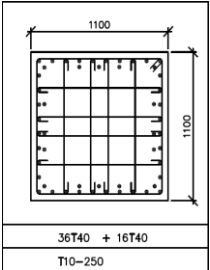
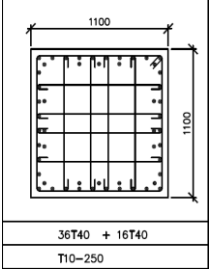
The blast effect analysis shall be done at a component level where each affected structural and non-structural component is individually analysed against blast. All assumptions adopted shall be clearly stated with appropriate explanation of why these assumptions were adopted (substantiated with relevant references, code of practices and standards, if applicable). All design parameters (e.g., materials properties, factors applied, etc.) used in the design shall also be clearly stated.

The CP (Blast) shall provide a detailed list of all the physical hardening/non-hardening measures so as to allow CPS to easily track the implementation of the various measures. A sample is as shown in [Table E](#) for reference.

Table E – Details of Physical Hardening/Non-Hardening Measures

Element Type/ID	Structural Dimensions	Threat Scenarios	Design Checks (Pass/Fail?)	Predicted Impacts/Consequences to the Structural Elements/CA	Proposed Hardening/Non-Hardening Measures Details	Measures To Be Implemented (Y/N/NA?)	Residual Risk For Measures Not Implemented
		<i>(List all threat scenarios)</i>	<i>(List down all the checks that had been done)</i>	<i>(You may copy directly from BEA, if there are no changes to the findings.)</i>			<i>(After implementation of the proposed measures and if there are still any residual risks, please indicate concisely in this column.)</i>

²⁶ The legend can be readily amended to reflect additional components not captured in current template.

<p>Column / 2A4</p>	<p>1,100mm x 1,100mm Column Height: 4m</p> <p>Main Rebars: 36T40 + 16T40 Links: T10-250 c/c</p> <p>X-Sectional Details</p> 	<p>250kg VBIED at 6.5m (along ABC Avenue)</p>	<p>Pass Breach, Spall & SDOF</p>		<p>Refer to footnote.²⁷</p>		
<p>Column / 1A3</p>	<p>1,100mm x 1,100mm Column Height: 4m</p> <p>Main Rebars: 36T40 + 16T40 Links: T10-250 c/c</p> <p>X-Sectional Details</p> 	<p>20kg PBIED at 0.2m (at screening station)</p>	<p>Fail Breach & Spall</p>		<p>Refer to footnote.²⁸ i.</p>		

²⁷ Not Required if the component was able to withstand the blast load, and no physical hardening measures are needed to be implemented, then just state "Not Required".

²⁸ i. CP (Blast) shall state the hardening measures (if any) and provide structural details of these hardening measures.
ii. CP (Blast) may wish to include technical specification of the proprietary materials/technology measures which are proposed for use.
iii. CP (Blast) shall state the likely residual risk (if any) faced by the affected assets within the building after implementation of the physical hardening measures.
iv. If no measures could be implemented to mitigate the risk(s), the CP (Blast) shall indicate reason(s) why this cannot be mitigated and the corresponding residual risks associated with this.
v. CP (Blast) shall proposed contingency plans to reduce the residual risks, if applicable. The relevant stakeholders' agreement on the above items are required to be sought and properly documented in this report.

3. The report should comprise, but not limited to, the above key items in separate chapters and should generally follow the order listed.
4. All recommendations proposed by the CP (Blast) have to be reviewed and accepted by the RP as the RP is presumed to be implementing all of the recommendations stated in the final SPP submitted to CPS.
5. Relevant documents and drawings shall be attached in the Appendix of the report for easy reference and a suggested list is as shown in Table F.

Table F – List of information²⁹ required in the Appendix

S/N	Description of Documents/Drawings
1	Site/Location Plan
2	Architectural Layouts and Elevations
3	Architectural Details e.g., opening sizes of doors, louvers, windows, etc.
4	Structural Layouts and Elevations
5	Structural Details e.g., dimensions and reinforcement details for columns, beams and slabs
6	Layout(s) showing the locations of critical assets and their respective standoff distances from the threat
7	Layout(s) showing the demarcated boundaries of public and restricted access areas
8	Drawing(s) showing all changes that are relevant to the SBD submission for the facility (applicable for A&A works and any SBD amendment submission)
9	Structural Hardening Details/Shop Drawings
10	Technical Specification of Proprietary Materials/Technology Measures
11	References, Code of Practices and Standards, where applicable
12	Supporting Documents/Certification and/or Performance Specifications for Blast Door, Blast Wall, Blast Valve, Vehicular Dynamics Assessment for Vehicle Security Barrier, etc.
13	For Structural Components: detailed calculations for all local and global checks
14	For Non-Structural Components (e.g., glazing, equipment, roller shutter, etc): detailed calculations that are relevant to justify its survivability
15	For Human Injury Prediction: detailed calculations that are relevant to justify its survivability
16	Analysis and results from design software

²⁹ Provide only those documents/drawings (NOT the entirety) that are relevant to this study. Drawings shall be provided in PDF format, A3 size with details clearly annotated. Reports and/or other kind of information shall be provided in PDF format.

REQUIREMENTS FOR SECURITY PROTECTION PLAN (SPP)

1 SPP Overview

- 1.1 The SPP documents all the security measures that will be implemented to mitigate the risk faced by identified critical assets against threats identified in the TVRA report.
- 1.2 The SPP is crucial in setting the record, outlining the importance of security for the Critical Physical Infrastructure, defining the scope of protection and critical assets, stating the Security Objective and aligning the Security Mitigation Measures to corresponding threats.
- 1.3 This section describes the minimum details required in a SPP report, as well as other required information. Should the SPP report contain additional items or security measures, the Competent Persons (CPs) shall furnish appropriate details to meet the above purpose.

2 Key Elements

- 2.1 In the SPP report, the following key elements are generally considered:
 - a. Introduction
 - b. Description of Protective Measures
 - c. Plans for additional measures during heightened threat conditions
 - d. Ballpark cost estimates for security measures and implementation timeline
 - e. Summary table of Mitigation Measures (SMM) based on layers of protection ([Table 1](#))
 - f. Residual Risk

3 Introduction

- 3.1 The introduction should contain the security objectives of the Security-by-Design (SBD) review for the Special Development/Special Infrastructure (SD/SI).
- 3.2 General information of the infrastructure should be added:
 - a. Brief description of the infrastructure,
 - b. location map/site layout with clear illustration of the roads adjacent/leading to the facility,
 - c. building footprint including perimeter line,
 - d. vehicular/staff/public accesses,
 - e. locations of critical assets, areas of mass congregation (if applicable),
 - f. key facilities that support the continued function of security measures,
 - g. staff/public car park, loading & unloading accesses/bays,
 - h. security control rooms,
 - i. restricted areas within building, etc.
- 3.3 The concept of protection such as Prevent, Deter, Detect, Delay, Deny and Response should be clearly mentioned in this section. Other concepts such as security zoning should also be mentioned in the SPP report.

- 3.3.1 The CP should apply the security zoning concept to control human movement within the infrastructure. Zoning allows staff, visitors, vendors, and others to reach their destinations without hindrance, and at the same time prevents their access to areas where they are not authorized to access. Controlling of access to each department inside an infrastructure will screen out undesirable visitors, reduce congestion, and help employees spot unauthorised persons.
- 3.3.2 The CP may illustrate how zoning design goals are accomplished through the use of unrestricted zones, controlled zones, and restricted zones. Some areas of the building may be completely unrestricted to persons entering the area during the hours of designated use. The design of unrestricted zones should encourage persons to conduct their business and leave the building without entering controlled or restricted zones. Examples of unrestricted zones might include lobbies, reception area, snack bars, and public meeting rooms. Examples of controlled zones might include administrative offices, staff pantry, security offices, office working areas, and loading/unloading docks. Restricted zones are essentially limited to designated staff. Particularly sensitive areas within restricted zones typically require additional access control as these might contain, for example, classified records, hazardous materials and cash.

4 Description of Protective Measures

- 4.1 The CP shall include all the proposed security measures in this section according to the category indicated in 4.2. to 4.5 (Structural hardening, Physical, Operational and Technological measures) to mitigate against the risk found in the TVRA.
- 4.2 Structural Hardening Measures
- 4.2.1 The CP shall provide the details for the structural hardening measures as mentioned in the table below.

Measure	Details Required
Structural components (e.g., columns, beams, walls, and slabs)	a. Mark out the locations of the critical assets, the structural components which require hardening, and the proposed structural hardening measures on architectural/structural drawings b. Physical dimensions and mechanical properties of component (e.g., elastic modulus, compressive and tensile yield and ultimate strengths, etc.) and its reinforcement (e.g., reinforcement steel, steel jacket, etc.), connection design and details, pre- and post-hardening. c. All other details relating to analysis of structural hardening design as stated in Annex D .

<p>Ground Shock protection</p>	<p>Based on the ground shock analysis in the BEA report, CP(Blast) will need to document the need for shock protection designs for all critical assets and its associated residual risks in the summary table below.</p> <table border="1" data-bbox="451 255 1353 880"> <thead> <tr> <th data-bbox="451 255 587 647">Critical Asset (CA)</th> <th data-bbox="587 255 751 647">Design Parameters for shock protection³⁰</th> <th data-bbox="751 255 924 647">CA Survivability (Y/N)³¹</th> <th data-bbox="924 255 1171 647">If CA fails, residual risk accepted by RP? (Y/N) If No, to submit all shock protection designs and calculations during CWC stage</th> <th data-bbox="1171 255 1353 647">Type of shock protection measures (shock isolator/hard mounting)</th> </tr> </thead> <tbody> <tr> <td data-bbox="451 647 587 719">CA 1</td> <td data-bbox="587 647 751 719">Vmax = Amax =</td> <td data-bbox="751 647 924 719"></td> <td data-bbox="924 647 1171 719"></td> <td data-bbox="1171 647 1353 719"></td> </tr> <tr> <td data-bbox="451 719 587 790">CA 2</td> <td data-bbox="587 719 751 790">Vmax = Amax =</td> <td data-bbox="751 719 924 790"></td> <td data-bbox="924 719 1171 790"></td> <td data-bbox="1171 719 1353 790"></td> </tr> <tr> <td data-bbox="451 790 587 880">CA X</td> <td data-bbox="587 790 751 880">Vmax = Amax =</td> <td data-bbox="751 790 924 880"></td> <td data-bbox="924 790 1171 880"></td> <td data-bbox="1171 790 1353 880"></td> </tr> </tbody> </table>	Critical Asset (CA)	Design Parameters for shock protection ³⁰	CA Survivability (Y/N) ³¹	If CA fails, residual risk accepted by RP? (Y/N) If No, to submit all shock protection designs and calculations during CWC stage	Type of shock protection measures (shock isolator/hard mounting)	CA 1	Vmax = Amax =				CA 2	Vmax = Amax =				CA X	Vmax = Amax =			
Critical Asset (CA)	Design Parameters for shock protection ³⁰	CA Survivability (Y/N) ³¹	If CA fails, residual risk accepted by RP? (Y/N) If No, to submit all shock protection designs and calculations during CWC stage	Type of shock protection measures (shock isolator/hard mounting)																	
CA 1	Vmax = Amax =																				
CA 2	Vmax = Amax =																				
CA X	Vmax = Amax =																				
<p>Glazing and Building Fabric</p>	<p>a. Mark out identified glazing and building fabric for strengthening on architectural drawings. b. Calculation showing the designs of the glazing/fabric system including framing details, anchoring details and structural support required.</p>																				

³⁰ Units of measurement for velocity (V) and acceleration (A) are mm/s and g respectively. All shock calculations shall be designed and endorsed by Professional Engineer.

³¹ CP(Blast) shall verify that the information is accurate and factual.

4.3 Physical Measures

4.3.1 The CP shall provide the details of the physical measures mentioned in the table below.

Measure	Details Required
Vehicle Perimeter Line	<ul style="list-style-type: none"> a. Mark out the locations of all Vehicle Security Barriers (VSBs) at the perimeter line on architectural drawings. Ensure that the drawings are detailed and clear enough for CPS's assessment of the continuity and consistency of the VSBs. b. Vehicle Speed Analysis (VSA), which identifies possible unobstructed vehicle paths towards the vehicular ingress and egress of the infrastructure, shall be conducted to determine the impact speed of vehicle and documented. c. Description of the type and crash-ratings of VSBs at the perimeter line e.g., wall, planter, bollard, gate, retaining wall, etc. If a low wall design or any similar structure is to be designed as a barrier, the CP shall provide structural drawings of the barrier, showing dimensions, the details of the reinforcement and the connection details. This design work shall not be outsourced to the construction vendor to carry out. d. Provide detailed justifications of using non-crash tested VSB as an effective measure against hostile vehicles, e.g. Reinforced-Concrete retaining wall, landscaping slope, etc. e. Ensure that proposed VSBs shall be crashed tested to ISO 22343-1, IWA 14-1 or ASTM F2656/F2656M or PAS 68 by an accredited test centre. All VSBs shall be independent and not integrated with any other fixtures (e.g., fence). Otherwise, the complete system of fixture embedded into the VSB must be crash tested to meet the above-mentioned standards by an accredited test centre. This is to maintain the crash rating for the crash tested VSBs. f. If crash-rated VSBs are not feasible or edge-to-edge distance between VSBs exceeds 1.2m due to site constraints, the SPP report must include the justifications and alternative solutions to mitigate against hostile vehicle.

Fence line	<ul style="list-style-type: none"> a. Mark out the location of the fence line on architectural drawings. Ensure that the drawings are detailed and clear enough for CPS's assessment of the continuity and consistency of the fence line. b. Provide the design specifications of the fence line, with details on the fence's anti-climb features (i.e., mesh size, material, type of top guards, etc.). c. Indicate the footing depth (to prevent tunneling attempts) and confirm that there is no foothold for intruder. d. Indicate the distance between the fence line and external fixtures (bus-stop, taxi stand, lamp post, sheltered walkway, trees, etc.) directly outside the facility and the recommended measures to mitigate against scaling of fence using these fixtures. e. If the fence serves the function of hostile vehicle mitigation, the crash-rating must meet the above-mentioned requirements for "Vehicle Perimeter Line" and included in the SPP report. f. Indicate whether grilles are installed to secure utility openings (e.g., drains) against intrusion into the facility. Provide specifications for these grilles and indicate which international anti-intrusion standards it meets.
Forced Entry (FE)	<ul style="list-style-type: none"> a. Mark out the FE measures and ensure that they are certified to FE standards stipulated in GEBSS. b. Perform vulnerability analysis on the FE risks for rooms or compartments housing the critical assets located adjacent to publicly accessible areas. c. Provide the design specifications of the wall, ceiling and floor slabs, door and locking systems with details on FE resistance features: <ul style="list-style-type: none"> i. Doors for critical asset rooms should be certified to EN 1630 or equivalent. The SPP report should include justifications for the proposed resistance time (of the certified door) and alternative solutions if unable to comply to the standard. ii. The adjacent wall(s) of critical asset rooms shall meet the minimum requirements of 150 mm thick reinforced concrete. iii. Grilles used to secure utility openings (e.g., ventilation openings etc.). d. The SPP report must include justifications and mitigation measures if windows are necessary due to operational requirements.

4.4 Operational Measures

4.4.1 The CP shall provide a list of the security measures required during times of normalcy. For each measure or plan, the CP shall provide a generic workflow of the measure/plan that describes the necessary general actions required and how any necessary security measure, supporting equipment and infrastructure provision are to be incorporated into the workflow. The CP shall also explain the rationale for the operational measures and how it reduces the risks faced.

4.5 Technological Measures

4.5.1 The CP shall provide details for the technological measures listed in below table. These are the minimum requirements for each measure. CP shall clearly explain its rationale, the key considerations, and how it lowers the risks.

Measure	Details Required
Video Surveillance System (VSS)	<ul style="list-style-type: none"> a. Mark out clearly the locations of all cameras (including cameras with Video Analytics (VA) capability) of the entire premises (i.e., perimeter, open spaces and roads, every level including rooftop and basement levels) in the architectural drawings. b. Provide key performance and technical information (i.e., types of cameras, image presentation, recording requirements, fields of view, coverage requirements) of the VSS. c. State the recommended features of the VSS e.g., the kinds of VA to be incorporated, location and period where VA will be armed, deployment of Pan-tilt-zoom (PTZ) cameras, Automatic Number Plate Recognition (ANPR) system, etc. d. Provide references to relevant standard or guidelines used in the design of the VSS³², if any.
Lighting	<ul style="list-style-type: none"> a. Lighting performance specifications (i.e., illuminance requirement) at required locations to facilitate surveillance and security screening operations, VSS monitoring/recording, etc. b. Provide references to relevant standard or guidelines used in the design of security lighting, if any.
Access Control System (ACS)	<ul style="list-style-type: none"> a. Mark out access control methods and authentication methods on architectural drawings e.g., card reader, mechanically locked doors/gates, electro-mechanical or electro-magnetic locked doors/gates, door contact sensors, turnstiles, etc. b. Explain the consideration for the recommended locking devices and its feature for security access card formats, locking mechanisms and fail-safe or fail-secure access. c. Provide references to relevant standard or guidelines used in the design of ACS, if any.
Intrusion Detection Systems (IDS)	<ul style="list-style-type: none"> a. Provide the type of detection systems deployed and location of deployment e.g., exterior (fence, gates, turnstile, etc.) and interior (door, windows within rooms) intrusion detection systems. The locations shall be marked out on architectural drawings. b. Provide the considerations for the selection of the IDS system. c. Provide the operating environment in which the systems have to operate in, as well as the performance specifications that they will have to meet. d. Provide references to relevant standard or guidelines used in the design of IDS, if any.

³² The proposed VSS should minimally meet the requirements in SPF's VSS Standard for Buildings.

Security Screening Systems	<ul style="list-style-type: none"> a. Mark out locations for personnel and vehicle screening areas, and the security screening systems. b. Specify the type of security screening systems deployed. c. Explain and illustrate clearly the sequences of ingress/egress for personnel and vehicle from main entrance through security screening point, including driver and passengers of vehicles.
Electronic Key Management System (EKMS)	<ul style="list-style-type: none"> a. Provide the location of the EKMS. b. Provide the details on the level of access for different categories of personnel working in the facility authorized to withdraw keys. c. Provide technical information of the EKMS (i.e., mode of authentication, authentication methods (e.g. Two-Factor Authentication), tamper-proof, type of security plugs, built-in video surveillance, etc.)
Security Integration Platform	<ul style="list-style-type: none"> a. Provide details of integration between different physical security systems such as VSS, access control and intrusion detection), modes of operation, and high-level network topology plans, if applicable. b. Provide the contingency plans for monitoring the individual security monitoring systems during platform failure. c. Provide details of the locations at which all security systems (e.g., VSS, IDS, ACS, screening systems, EKMS, etc.) are controlled and monitored. d. [For Addition and Alteration (A&A) works only] Assessment on the need to upgrade part or all existing systems, and the compatibility of new systems with existing systems.

5 Plans for additional measures during heightened threat

- 5.1. The CP shall state any additional measures during heightened threat such as the process and procedure of the different threat level, from the start to the end stage of the heightened threat, including the preparation for heightened alert.
- 5.2. For each measure or plan, the CP shall provide a generic workflow of the measure/plan that describes the necessary actions required.

6 Ballpark cost estimates for security measures and implementation timeline

- 6.1. The CP shall include the breakdown cost of the proposed security mitigation measures including cost estimate of the hardening measures required.

7 Workplace Shelter

- 7.1. If a workplace Shelter is required, the RP shall provide the Concept of Operations (CONOPS) and contingency measures that will be put in place.

8 Summary table of Mitigation Measures (SMM) based on layers of protection

- 8.1. The CP shall provide a summary table of all the physical, operational/human and technological measures that will be implemented so as to allow CPS to easily track the implementation of the various measures. A sample can be found in Annex E1.

9 Residual Risks

- 9.1 The CP shall include in the SPP, an articulation of the likely residual risks faced by the critical assets within the infrastructure after the implementation of the security measures. This should be done in consultation with the RP and Sector Lead (SL), if applicable. The final residual risk should be clearly documented in the SPP and accepted by the RP.

1. The Security Protection Plan (SPP) details the protective measures to be put in place to mitigate the vulnerabilities of identified critical assets of an infrastructure, corresponding to threats identified in the Threat, Vulnerability, and Risk Assessment (TVRA) report.

2. To facilitate the SBD review, the CP should ensure that the SPP has comprehensively covered the following key areas:
 - a. Executive summary

 - b. Introduction
 - i. Security objectives of SPP

 - ii. General information of the infrastructure
 - a) Brief description of the infrastructure
 - b) Location map/site layout with clear illustration of the roads adjacent/leading to the facility
 - c) Building footprint including perimeter line, vehicular/staff/public accesses, staff/public carpark, loading & unloading accesses/bays, security control rooms, restricted areas within building, locations of critical assets, areas of mass congregation, etc.

 - iii. Concept of protection
(This section refers to the multi-layered protection concept of Prevent, Deter, Detect, Delay, Deny and Response)
 - a) Approach/Underlying parameters for risk assessment
 - b) Protection criteria
 - c) Security zoning
 - d) Assumptions

 - c. Description of Protective Measures
 - i. Physical/Structural measures for [Type of Threats]
 - a) Existing situation, vulnerabilities, impacts and consequences
 - b) Recommended measures
 - c) Layout, installations and specifications

 - ii. Operational measures for [Type of Threats]
 - a) Existing situation, vulnerabilities, impacts and consequences
 - b) Recommended measures
 - c) Deployment plans and security communication
 - d) Operational plans
 - e) Standard Operating Procedures

 - iii. Technological measures for [Type of Threats]
 - a) Existing situation, vulnerabilities, impacts and consequences
 - b) Recommended measures
 - c) Deployment plans and system specifications

 - d. Plans for additional measures during heightened threat
 - i. Scenarios/times of heightened threat
 - ii. Recommended measures

- iii. Deployment plans
 - iv. Operational plans
 - e. Ballpark cost estimates for security measures and implementation timeline
 - f. Summary table of Mitigation Measures (SMM) based on layers of protection (Table 1)
 - i. Threat specification and payloads (if applicable)
 - ii. Modus operandi
 - iii. Location of critical assets
 - iv. Consultant's assessment
 - v. Recommended measures
 - vi. Limitations, if any
 - g. Residual Risk
 - i. Articulation of the likely residual risk faced by the affected assets within the infrastructure after the implementation of the security measures.
 - ii. Proposed contingency plans to reduce the residual risks, if applicable
 - iii. Acceptance of residual risk by RP in consultation with SL if applicable
3. The report should comprise, but not limited to, the above key items in separate chapters and should generally follow the order listed.
 4. For each measure, the CP shall provide a generic workflow of the measure that describes the necessary general actions required and how any necessary supporting equipment and infrastructure provisions are to be incorporated into the workflow. The CP shall also explain the rationale for the measure and how it reduces the risks faced.
 5. The CP shall provide a summary list of all the measures to allow CPS to easily track the implementation of the various measures. A sample is shown on Table 1.
 6. All recommendations proposed by the CP have to be reviewed and accepted by the RP as the RP is presumed to be implementing all of the recommendations stated in the final SPP submitted to CPS.

DOCUMENTARY SUBMISSION BEFORE AND DURING CONSTRUCTION

1. Requirements

1.1 The submission of required documents aims to ensure that security protective measures such as structural hardening have been incorporated into the construction phase. The Competent Person (Blast) (CP(Blast)) shall work closely with the Responsible Person (RP) and the Qualified Persons (QPs) to ensure that Physical Hardening Measures (PHMs) are implemented as spelt out in the approved Security Plan (ASP).

1.2 The CP must verify that the method statements, shop drawings, materials and workmanship specifications submitted by the vendor/contractor in the awarded construction tender are in accordance with the ASP. If the contractor proposes any deviation from the security measures as spelt out within the ASP, the CP shall advise the RP on whether the deviation is acceptable. If the deviation results in major changes, the RP shall inform CPS immediately and there may be a need to submit an amendment to the ASP in the manner spelt out in [Annex G](#).

1.3 The CP shall submit the construction schedule for the installation of structural hardening measures. CPS will assess the need to visit the site to inspect the implementation of these structural hardening measures. Details required to be submitted by CP(Blast) before constructions and requirement to be fulfilled by CP(Blast) during construction are listed in the tables below.

Before Construction

Documents	Details required to be submitted by CP (Blast)
Site Inspection Schedule	The site inspection schedule (in Gantt Chart format) indicating all key milestones for inspections on related structural hardening elements shall be submitted not less than 1 month prior to the start of the construction.

During Construction

Documents	Requirement to be fulfilled by CP(Blast)
Site Inspection Reports	The following documents shall be submitted during construction: <ol style="list-style-type: none"> CP (Blast) shall be present during all key inspections dates as stated in the site inspection schedule. CPS may be present for the inspection; After the site inspection, site inspection reports (<i>with appropriate site photos</i>) that detail the proper implementation of the structural hardening measures shall be documented and submitted during CWC. These reports must be endorsed by the CP (Blast).
Documentation for major changes	If there are major departures or deviations from the ASP, documents (drawings, calculations, FEA models, etc.) shall be submitted to CPS for approval.

AMENDMENTS TO APPROVED SECURITY PLAN

1. Under the IPA, the Commissioner may, at any time and through a written notice to the Responsible Person (RP), require amendments to the Approved Security Plan (ASP). The RP must submit the revised plan for Commissioner's approval in the required form and manner and within the timeframe specified in the notice.
2. The RP may, at any time, apply for the Commissioner's approval to amend the ASP. The application must be submitted in the required form and manner, along with the amended security plan and any additional information or supporting documents as required by the Commissioner³³.
3. The RP is responsible for implementing, or ensuring the implementation of, all security measures stated in the ASP. Any modification that affects the implementation of these security measures may necessitate an amendment to the security plan.
4. Any changes that may affect the risk rating of the critical assets will likely require an amendment to the Security Plan. Below are some possible scenarios (non-exhaustive) that could necessitate such amendments.
 - a. New threat scenarios: New building developments (e.g., underground connection to public transport, repurposing of spaces such as converting staff carpark to public carpark) may introduce threats that were previously not considered to the critical assets;
 - b. Changes that affect the security measures: The list of existing and proposed security measures is a key factor in Vulnerability Analysis e.g., a crash-rated fence line is critical in preventing a VBIED threat from entering the site. If, during construction, the RP discovers that ground conditions prevent the installation of a complete crash-rated fence line, the risk rating for the affected critical assets will be impacted, as a VBIED can now penetrate the site;
 - c. Changes that affect Consequence/Impact Analysis: Certain modifications to key structural components or protective hardening measures may impact the risk rating of critical assets and necessitate amendments to the ASP. These include:
 - i. Structural modifications: Changes to columns, beams, slabs, load bearing walls, or rebar configurations that support critical assets may affect the overall stability of the structure. Unlike conventional design, adjustments to structural sizes or reinforcement directly impact the building's resistance to threats.
 - ii. Loss of redundancy: Redundant systems (e.g., cooling system, power supply) are integral to risk mitigation. If site constraints prevent the implementation of planned redundancy, the impact analysis and risk rating must be reassessed.
 - iii. Protective Hardening Limitations: Security-enhancing measures (e.g., blast resistant reinforcements, crash rated barriers) are critical for mitigating structural vulnerabilities. If ground conditions or design limitations prevent their installation, the overall risk to critical assets increases.

³³ Section 37(3) of Infrastructure Protection Act

- d. For significant structural or security related changes, the CP (Blast) must collaborate with the Qualified Person (QP) and CP (Security) to assess whether the protective systems remain effective. If the changes impact the security risk levels, the RP must consult CPS early to determine whether an amendment to the ASP is required.
5. Amendment to ASP is generally not be required for the changes below (see [Table 1](#)):
- Minor changes that neither affect Security Mitigation Measures nor the key structural elements;
 - The effects of the changes are localized in nature and do not require a re-design of the Security Mitigation Measures or key structural elements.

Table 1: List of Works that do not Require Amendment to ASP (not exhaustive)

Type	Examples
Temporary Works	<ul style="list-style-type: none"> Construction of temporary buildings (e.g., builders' working shed, site office, contractors' hut, shelters, platforms, scaffoldings or hoarding areas, etc.) that will be removed upon completion. Temporary works (e.g. struts, king posts, retaining structures, etc.) installed during construction that will be removed upon completion.
Internal partitioning, re-arrangement of office spaces in part of a building that does not contain a critical asset	<ul style="list-style-type: none"> Redesigning of office spaces with gypsum boards and/or other non-load bearing structures (e.g., masonry/partition walls, etc.) in part of a building that does not contain a critical asset.
Installation of machinery	<ul style="list-style-type: none"> Installation of new machineries (non-critical asset) that do not affect security risk profile of the infrastructure.
Change of brand of security products	<ul style="list-style-type: none"> Change of brands of security products with equivalent or higher specifications due to availability or site constraints.
Alteration and Addition Works	<ul style="list-style-type: none"> Structural works consisting of repairs, alterations and additions to an existing building which do not materially affect the key structural elements of the building under all the identified threat scenarios e.g., changes of rebars diameter and spacing but the overall rebar area remains unchanged.

6. The RP and CPs should consult CPS early to determine whether the proposed changes meet the criteria above. For amendment to ASP, the CPs will be required to update the relevant sections of the security plan and highlight the new residual risks where applicable.

1. This appendix outlines the necessary information to be included in the report for amendment of ASP.
2. The amendment report shall detail changes that affect the risk profile or security measures. It must incorporate relevant elements from the ASP (TVRA, BEA, SRS and SPP).
3. The CP must ensure that the amendment report covers the following sections:
 - a. Executive summary: A brief overview of the amendments, summarizing key changes and their rationale.
 - b. Background
 - i. Security objectives of the SD/SI: Outline the security objective of the SD/SI
 - ii. Scope of the ASP: Define the coverage of the ASP
 - iii. Date of ASP: Indicate when ASP was granted
 - iv. Reason for the amendments: Justify why the changes are necessary (e.g., new threat scenario, structural modification, etc.)
 - v. Summary table of the amendments ([Table1](#))

Table 1: Summary table of amendment

S/N	Existing Plan	Details of changes	Cas affected by the change	Risk Assessment	Proposed change to the security measures
1	e.g. Para x page x TVRA/SPP, layout, etc	Change in the column size due to X reason.	CA1 affected	Change in risk score (reason)	Additional PHM for affected area
2					
3					

- c. Amendment³⁴
 - i. Overview of the changes to physical hardening or security measures
 - ii. Approved security measure to mitigate type of threat in the ASP
 - iii. Risk assessment of proposed Security Plan (TVRA/BEA)
 - (a) Justification for changes to the TVRA risk score and affected critical assets. Supporting evidence should be provided in the Threat,

³⁴ The structure of Section C should be repeated if there are multiple amendments.

Vulnerability, Consequence (TVC) table, including changes to the security plan and BEA.

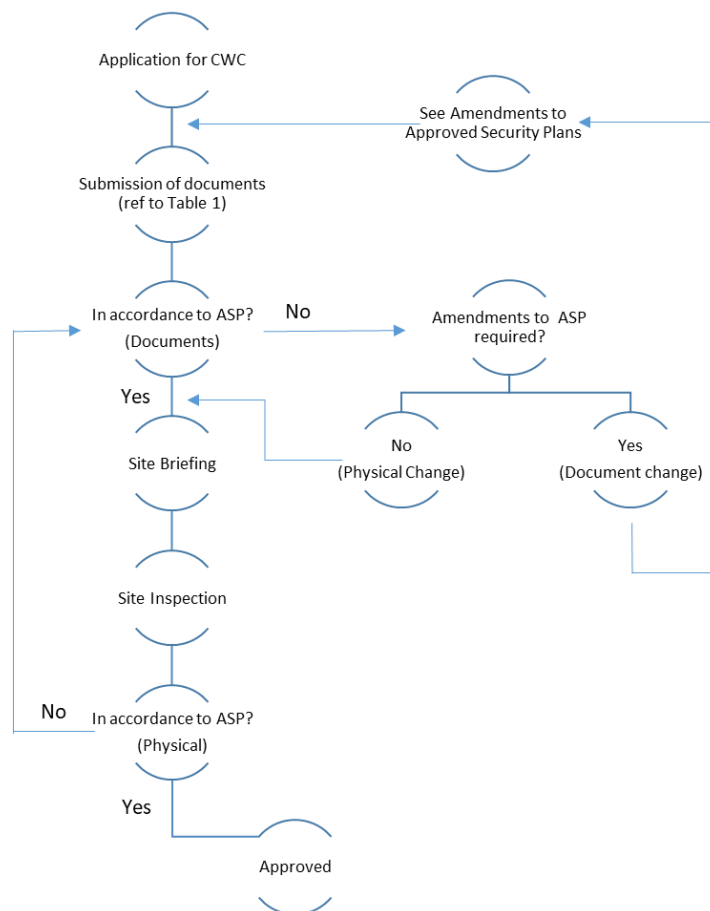
- (b) Explanation of the remaining risks faced by the affected assets within the infrastructure due to changes in security measures
 - iv. Proposed additional security measures to mitigate increased security risks or type of threat (SRS/SPP), if applicable.
 - (a) Layout of affected area
 - (b) Installation or changes in security measures
 - (c) Specifications of proposed measures
 - (d) Other Requirements, as stated in SPP
 - v. Proposed contingency plans to reduce the residual risks, if applicable
 - vi. Acceptance of new residual risk
 - d. Conclusion
2. The report should include, but is not limited to, the key items listed above, with each section presented as a separate chapter. The report should generally follow the prescribed order to ensure clarity and consistency.
 3. The CP shall provide an updated summary list of all approved and proposed security measures, allowing CPS to easily track the implementation. The summary should:
 - a. Consolidate all security measures, including those introduced in the amendment report.
 - b. Clearly indicate the security measures that are being removed using strikethrough formatting.
 - c. Reference [Table 2](#) for a sample on how this summary list should be presented.
 4. All recommendations proposed by the CP must be reviewed and accepted by the RP. The RP is responsible for implementing all the approved recommendations stated in the amended ASP submitted to CPS.

REQUIREMENTS FOR APPROVAL OF CERTIFICATE OF WORKS COMPLETION

1. Introduction

- 1.1 The Certificate of Works Completion (CWC) process certifies that the security measures stated in the approved Security Plan (ASP) have been implemented before or upon the completion of specified works. Upon the completion of specified works, the Responsible Person (RP) is required to submit the application for approval of CWC to the Commissioner.
- a. If the works require a Temporary Occupation Permit (TOP) or Certificate of Statutory Completion (CSC) from the Building and Construction Authority (BCA), it cannot be obtained without an approved CWC.
 - b. If the works do not require a TOP or CSC from BCA, the CWC must be submitted to the Commissioner for approval within 10 working days after the completion of specified works.

2. CWC Process Flowchart



3. Documentary Requirements

- 3.1 The RP should submit the application for approval of CWC with the supporting documents mentioned in **Table 1** to show that the measures have been implemented in accordance with the ASP.

Table 1: List of documents required for approval of CWC

Documents	Details Required	Documents to be arranged in the folders for submission/ Responsible Party
Application Form	1. Application form for approval of CWC by RP	1. Main Document
CWC with Summary Table of Mitigation Measures	1. CWC by CP(Security) and CP(Blast): a. Declaration that all design checks have been done in accordance with all relevant and prevailing codes and references; and b. Declaration that all protective security measures have been implemented according to the ASP and approved amendments, if any. 2. Summary table of mitigation measures as stated in the ASP, signed by CP(Security) and CP(Blast).	
Checklist of the Works Proposed in the SPP and Status of Completion	1. All security measures stated in the SPP should be reflected in the checklist. For example, security layer 1, layer 2, etc.	
Physical Measures	1. Crash-rating test certificate by accredited test centre for all crash-rated vehicle security barriers, including perimeter low wall with or without integrated anti-climb fence. 2. Forced Entry (FE) resistant components' test certificate by accredited test centre, including door and lock systems 3. Layout of all physical protective measures such as Hostile Vehicle Mitigation (HVM) ³⁵ measures, FE protection ³⁶ , fence line ³⁷ , etc.	2. Physical Measures
Operational Measures	1. <u>Workplace Shelter (if applicable)</u> Location of Workplace Shelter, details on In-Place Protection measures and operational manual on the proper use of Workplace Shelter.	3. Operational Measures
Maintenance Regime	1. Maintenance plans for all structural/physical protective solutions selected for implementation. The maintenance plans are to be provided to the RP for	4. Maintenance Regime

³⁵ CP(Security) to submit Crash Test Certificates for the HVM measures installed at the facility. If it is a system of fence embedded into low wall, the Crash Test Certificate should be for the full system. CP(Security) to ensure that the HVM measures are constructed according to OEM's method of installation.

³⁶ For FE protection, CP(Security) to submit Test Certificates of the product to confirm that it is tested to FE standards.

³⁷ For fences, CP(Security) to submit the finalized construction drawing and indicate actual location of installation.

	long-term maintenance of the physical protective solutions implemented.	
Test Certifications and Testing and Commissioning Reports	1. Relevant testing and commissioning reports (e.g., OSAT reports) and <u>testing certifications</u> to confirm that the implemented physical protective/technological security measures have met the required performance and technical specifications (signed off by CP(Security)), and <u>as-built drawings</u> .	CP (Security)
	2. The RP and CP(Security) shall also provide the following documents, where applicable: <ul style="list-style-type: none"> a. System Integration platform (if any): <ul style="list-style-type: none"> i. High level architecture of the system integration platform including the integration with various physical security systems and sensors. ii. Illustrate how security system status or alerts are displayed in system integration platform. iii. For Video Surveillance System (VSS) with Video Analytics (VA), provide the system notification logs and text notification logs (if any) that are sent to the assigned security personnel upon a VA alarm activation. b. Security screening equipment and the security operations manual, confirmation for security manpower and test certifications for hand-held/walk through detectors/X-ray machines/ Under Vehicle Screening System, etc. c. Testing results of the VSS, Access Control System (ACS) and Intrusion Detection Systems (IDS) activations along the perimeter line, all ingress and egress points (including gates and turnstiles), critical areas, security screening areas. For unmanned facility, tests should include alarm detections in both remote and off-site monitoring centres. d. System notification logs and text notification logs (if any) that are sent to the assigned security personnel upon a VA alarm activation. 	CP (Security)
	3. Material test certificate to ascertain that the actual material strength has achieved their design strength e.g., mill certificate, cube/cylindrical test, etc.	CP (Blast)
	4. Strength test of commercial products to ascertain that the actual material strength has achieved the desired outcome stated in the technical specification	CP (Blast)
Systems Specifications	1. <u>VSS, ACS, IDS, Electronic Key Management System (EKMS)</u> Detailed documentation of system specifications of the security systems (e.g., Brochures, and technical data sheets)	CP (Security)
	2. <u>Commercial Products</u>	

	Documentation proofs that all commercial products are installed according to vendors' requirements.	CP (Blast)								
Layouts/Photos	1. <u>Perimeter Line and Building Compound</u> a. Layout of multi-zone FIDS e.g., fibre optics/photo beam system, etc.	CP (Security)								
	2. <u>VSS</u> a. Layout of CCTV cameras b. Actual images taken from CCTV's field of view with accordance with the ASP. c. For cameras equipped with VA, minimally to provide actual images during night hours that illustrate the VA capabilities to detect intrusion from the furthest field of view.	CP (Security)								
	-									
	3. <u>ACS/ IDS/ EKMS</u> Layout of security zoning, location of ACS (Card reader, Electro-mechanical lock, EM lock, push button, break glass, etc.), IDS (magnetic door contact, motion sensors, etc.) and EKMS.	CP (Security)								
	4. <u>Physical Screening System</u> Layout of personnel and vehicular screening system (hand-held/walk through detectors/X-ray machines/ Under Vehicle Screening System, etc.).	CP (Security)								
5. <u>Physical Hardening Record Plans</u> Physical Hardening Record Plans (final Version, with CP(Blast)'s endorsement). This set of drawings shall be prepared as close as possible to the "As-Built", with minimum or no differences at all. It shall include all approved physical hardening measures details, approved deviations and amendments details, and other essential structural details. If there is no physical hardening measure implemented, submission of such drawings will not be needed.	CP (Blast)									
Site Inspection Reports	1. Site inspection reports (with appropriate site photos) shall capture the proper implementation of the structural hardening measures. CP(Blast) shall endorse these reports.	CP (Blast)								
	2. Shock protection a. Provide details on shock protection for all critical assets in the table below, if applicable.	CP (Blast) and Professional Engineer								
	<table border="1"> <thead> <tr> <th>CA</th> <th>Design Parameters for shock protection³⁸</th> <th>If CA fails, residual risk accepted by RP? (Y/N) If No, to submit all shock protection designs and calculations</th> <th>Type of shock protection measures (shock isolator/ hard mounting)</th> </tr> </thead> <tbody> <tr> <td>CA 1</td> <td>Vmax =</td> <td></td> <td></td> </tr> </tbody> </table>	CA	Design Parameters for shock protection ³⁸	If CA fails, residual risk accepted by RP? (Y/N) If No, to submit all shock protection designs and calculations	Type of shock protection measures (shock isolator/ hard mounting)	CA 1	Vmax =			
CA	Design Parameters for shock protection ³⁸	If CA fails, residual risk accepted by RP? (Y/N) If No, to submit all shock protection designs and calculations	Type of shock protection measures (shock isolator/ hard mounting)							
CA 1	Vmax =									

³⁸ Units of measurement for velocity (V) and acceleration (A) are mm/s and g respectively. All shock calculations shall be designed and endorsed by Professional Engineer.

	Amax =			
CA 2	Vmax = Amax =			
CA X	Vmax = Amax =			
<p>All shock protection designs and calculations are to be endorsed by the Professional Engineer, if applicable.</p> <p>b. Certification of supervision for installation of shock protection designs, if applicable.</p>				
				Professional Engineer

3.2 For Purpose-built Shelters, the RP and CP shall refer to [Annex J](#) for the additional requirements pertaining to the testing and commissioning, and CWC.

4. Site Briefing and Inspection

4.1 A joint site briefing and inspection with CPS should be arranged once all documents are in order. The site briefing should clearly articulate the work done from the time the Security Plan was approved to the completion of the specified works. To avoid delays to the approval of CWC process, any non-compliance found during the site inspection should be rectified or responded to within 10 working days with supporting documents submitted to CPS.

5. Approval for CWC

5.1 After the CWC requirements have been fulfilled, CPS will take about 20 working days to process the approval of CWC application.

INFORMATION SECURITY

1 Introduction

1.1 Sensitive information regarding infrastructure security measures and vulnerabilities must be safeguarded against unauthorised access and disclosure, whether accidental, or motivated by malicious intent. If sensitive information about implemented security measures falls into the wrong hands, it affords malicious actors the ability to counter and undermine the very security measure put in place to defend against them. Therefore, information security is imperative to the protection of infrastructure. It is important for the Responsible Person (RP) to have, and to enforce in others, an information security conscious mindset when handling such sensitive information.

2 Information Transfer

2.1 Information is most susceptible to unauthorised access and disclosure when it is transferred and duplicated. From tendering to the end of the Security-by-Design (SBD) process, there will be ongoing exchanges of information between parties such as CPS, RP(s), Competent Person(s) (CP(s)), consultants, construction, and architecture teams, etc. These transfers or storage of information can be either in electronic (emails, PDFs) or physical form (paper documents). The following diagrams broadly show the information transfers during the SBD process:

Fig. 1: Tender Stage

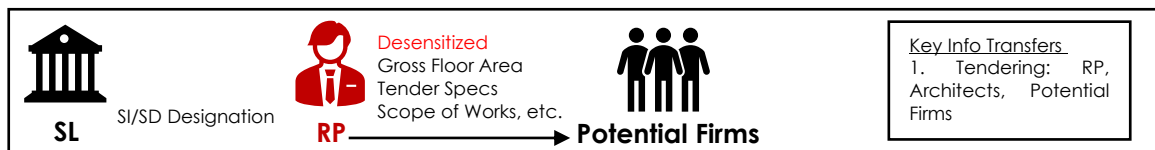


Fig. 2: Kick Off Meeting (KOM) to Approval of Security Plan Stage

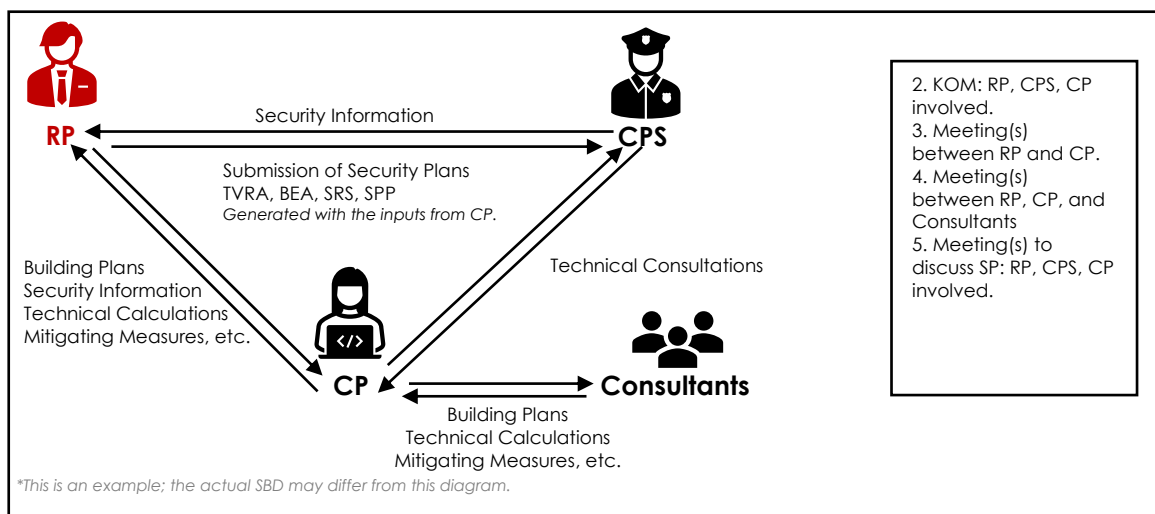
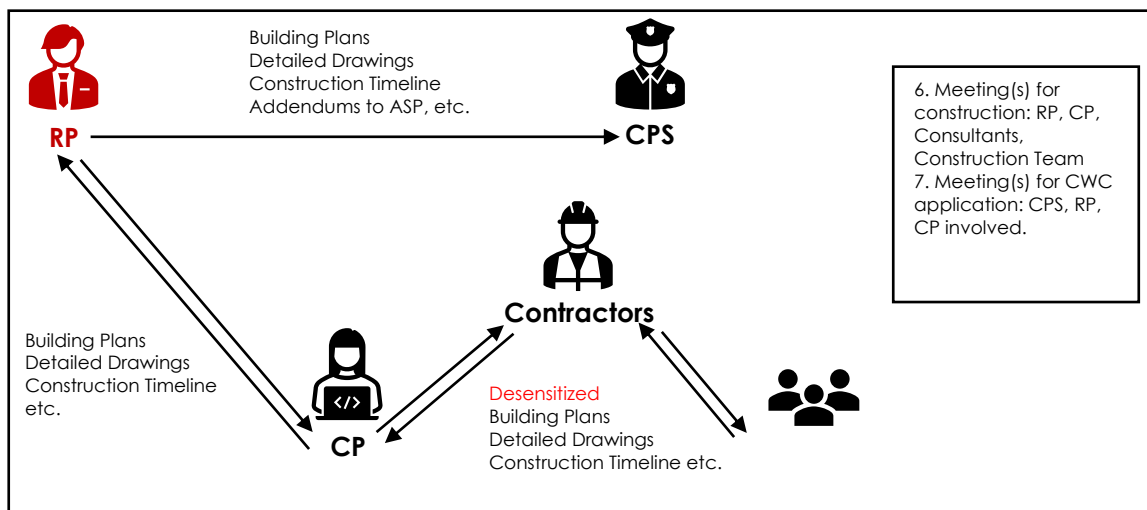


Fig. 3: Construction to Certificate of Work Completion (CWC) Stage



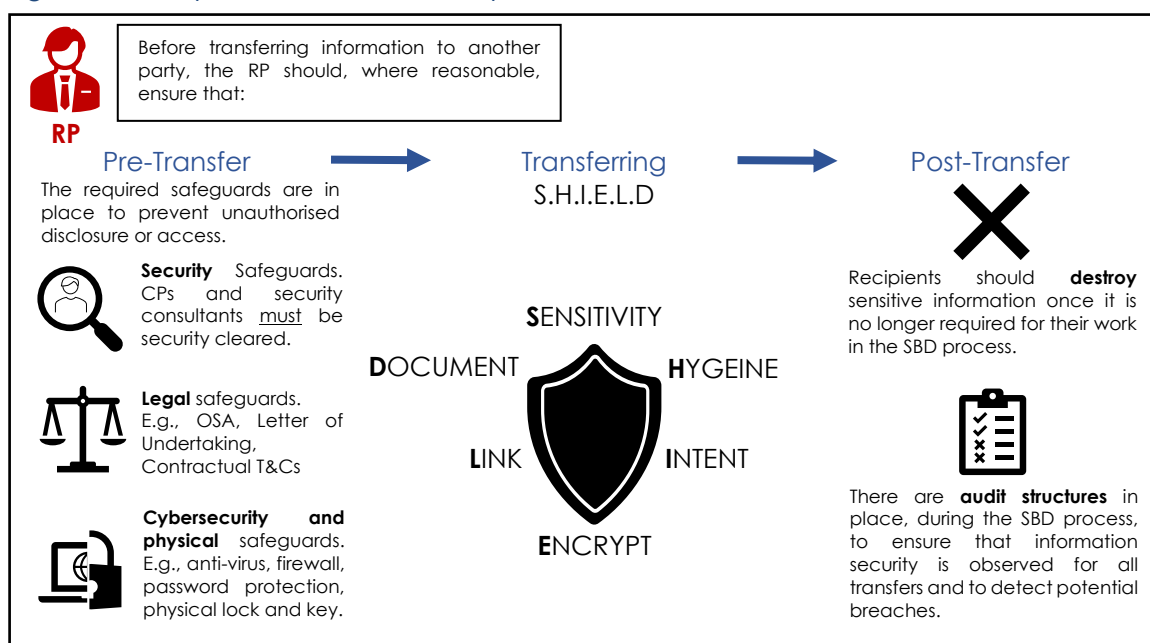
2.2 As shown in Fig. 2 and 3, there are many different stakeholders involved, both government and private sector parties, who come into and leave the SBD process at different stages. These arrangements result in numerous and concurrent instances of information transfer.

3 Best Practices for Information Security

3.1 The RP is the source of all information regarding the Special Development/Special Infrastructure (SD/SI); therefore, it is the RP's duty to ensure that the information disbursed is then subsequently protected.

3.2 These "best practices" are **strongly recommended** for ensuring information security. The best practices are split into different stages of information transfer: pre-transfer, transferring, and post-transfer.

Fig. 4: Summary of Information Security 'Best Practices'



4 Pre-Transfer

- 4.1 Before transferring any information, the RP should, as far as reasonable, ensure that these measures are in place:

Security Safeguards

- 4.2 The RP should ensure that any recipient of sensitive information has been security screened. Therefore, RP should pre-identify and notify CPS of the individuals who will be handling sensitive information and who will, therefore, require security screening. This applies to the CP(s) and any security consultants hired. RPs must wait for CPS's notification of security clearance for such individuals before transferring any sensitive information to them.³⁹

Legal Safeguards

- 4.3 The RP should ensure that there are legal safeguards in place to deter the recipients from unauthorised disclosure. This may take different forms for different recipients and in different stages of the SBD. Some common examples of legal safeguards include:

- i. Official Secrets Act (OSA)
For RPs from government agencies, the OSA can be used to criminalize the unauthorised disclosure of information from SBD processes for government SI/SD.
- ii. Contractual Terms and Conditions
RPs can also use legal safeguards in the form of contractual Terms and Conditions (T&Cs). These T&Cs can be written as a clause in the employment contract for the information recipient. Some common examples where such T&Cs can be used:
- Contract for hiring the architect firm, construction team, etc.
 - Legally binding letters of undertaking on information security*.
- *RP should seek proper legal advice when drafting.*

Cybersecurity and Physical Safeguards

- 4.4 The RP should ensure that there are appropriate cybersecurity and physical safeguards in place to deter and prevent unauthorised access by third parties. Safeguards can vary across projects. The RP may consider more drastic safeguards for highly sensitive projects. Some common examples of cybersecurity and physical safeguards include:

- i. Anti-virus software, firewall, password protection for devices, etc., that are updated when required.
- ii. Keeping devices or physical copies of SBD paperwork under lock and key or within a secured room.
- iii. For highly sensitive projects, safeguards can include restricting access to sensitive documents to within a particular secured room onsite and ensuring that these documents are not accessible via the internet.

- 4.5 The RP should reasonably ensure that these safeguards are in place, both for themselves and for the recipients of the information.

³⁹ More information can be found on the SPF website, including the requirements for CPs and a list of pre-cleared CPs.

5 Transferring (S.H.I.E.L.D)

- 5.1 The RP should keep in mind these principles when transferring information to others, whether by electronic or physical means.

Sensitivity: Separate sensitive and non-sensitive information and desensitize where possible

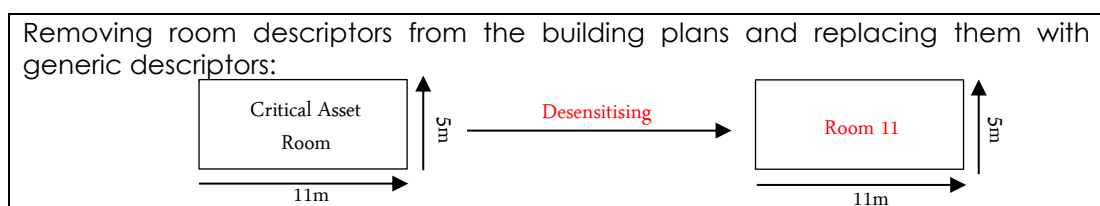
- 5.2 It is important to maintain a distinction between sensitive and non-sensitive information, not all party need to be privy to sensitive information. Sensitive information can be understood as information about security measures or their implementation. It is recommended that sensitive information be kept only within security cleared individuals (RP, CP, CPS). The table below provides an example of how information can be classified as 'sensitive' or 'non-sensitive':

Sensitive Information	Non-Sensitive Information
Details and rationale of the security measures. Example: Where CCTVs will be located, where the critical assets are kept.	Administrative/Construction Information Example: Construction Schedule, feasibility plans, Architecture Drawings.
Considerations: The information can be used by malicious actors to undermine the security measures by planning countermeasures.	Considerations: Such information may be intended to be kept private, but unauthorised disclosure is unlikely to affect the effectiveness of the security measures.

- 5.3 Sensitive information should be **desensitized** before sending to non-security cleared individuals as these individuals pose an unknown risk of compromising the information they receive. Examples of transfers where the information must be desensitized:

- i. Desensitizing information before transferring to bidding firms during the tendering stage.
- ii. Desensitizing information before transferring to construction teams.

- 5.4 Desensitizing includes replacing sensitive information with generic terms, removing sensitive information where it is not required and providing the minimal information necessary. Example:



Hygiene: Maintain good email hygiene

- 5.5 Email hygiene refers to the measures and practices that individuals can adopt to maintain a clean, secure, and efficient "email ecosystem". Given the widespread use of email for communication between the different parties, and the prevalence of email-based cyber threats, email hygiene is essential to protect against phishing, malware, and other email-borne attacks. Some principles of good email hygiene include, but are not limited to:

- i. Ensure that the recipient list is regularly curated to avoid sending information to unintended recipients.
- ii. Do not open suspicious links. Report and block the sender, then delete the suspicious email from the inbox.
- iii. Avoid forwarding long email chains when only the latest message is of importance. There may be sensitive information only meant to be kept between the initial parties contained in the earlier emails.
- iv. Only use the email address for work purposes, avoid cluttering the inbox with advertisement emails/social media alerts, etc.

Intent: Transfer information on a “need-to-know” basis

- 5.6 The RP should only send information if it is required by the recipient to perform their role, or on a “need-to-know” basis. The RP should have a good grasp of each party's involvement in the construction of the SD/SI and transfer information only based on the recipient's need for job completion. Therefore, it is also a good habit to separate the recipients where possible, using private chats or emailing individually, when sending sensitive information, to minimize the likelihood of unintended recipients and unauthorized disclosures.
- 5.7 As mentioned above, the RP should only send sensitive information to pre-identified security cleared individuals and desensitize the information when it is required by parties that are not security cleared. For example, for Design-Build projects, where the CP may be engaged by the contractor on behalf of the RP, communication of sensitive information in the security plan should be maintained directly between the RP, the CP and CPS only. Only information that the contractor needs to know (e.g., necessary for construction) should be released to the contractor by the RP/CP.

Encrypt: Encode and protect sensitive information

- 5.8 Encryption ensures that even if the document is intercepted by unauthorized third parties, it remains unreadable and confidential. There are several ways to encrypt information, with encryption software commercially abundant and usually integrated into devices and software such as email platforms and file directories. Additionally, sensitive information should be safeguarded using password protection. The RP should ensure that passwords are complex and unique, avoiding obvious and predictable combinations. Such passwords should also be sent in a separate message and/or channel.
- 5.9 If sensitive information is contained on a physical document, there should be additional care to ensure that it reaches the intended recipient. This can mean that such documents should be delivered personally instead of through commercial postal services.

Link: Choose the appropriate link for transfer

- 5.10 “Link” refers to the modality of transferring information. Choosing a suitable link may mean that the information is better safeguarded either because of increased protection or by minimizing unintended recipients. For example, messaging groups are suited for transferring non-sensitive information to a big group fast, while emails are suited for transferring sensitive information, requiring accountability, to a limited number of recipients. The RP may also choose a physical document as a ‘link’ when the information is highly sensitive and not suitable for ‘links’ that leave online traces.

Document: Track (document) sensitive information transfers

- 5.11 The RP should keep a log of who the information was sent to and the purpose for which it had been sent. Ideally, this would be done even for repeat recipients. Having an updated log of information transfers would help the RP maintain a clear oversight over

the information shared. In the event of unauthorized access or disclosure, this log can help the RP identify where and when the information was compromised.

6 Post-Transfer

6.1 RPs should ensure that the information is safeguarded post-transfer by:

Requesting destruction once information is no longer required.

6.2 It is recommended that the sender requires sensitive information to be destroyed once the SBD process is completed, or once it is no longer required by the recipient on a “need-to-know” basis. For information in electronic format, this would be permanent deletion. For information contained in physical documents, this can mean shredding and proper disposal or even returning to the original sender. This should be legally mandated through inclusion in a clause contained within a contract or a Letter of Undertaking and getting the recipient to make a declaration. For example:

Clause xx: Upon the attainment of the CWC or requested by <RP>, <receiving party> shall promptly and securely destroy all copies of classified material provided by <RP>. The destruction shall be conducted in a manner that ensures the information cannot be reconstructed or recovered. *

**For illustrative purposes only, RP should seek proper legal advice when drafting.*

6.3 RPs can also request for legally binding declarations from the recipients of sensitive information stating that they have returned or removed all copies of the information from their possession.

Incorporating audit structures.

6.4 Where possible, RPs should also undertake some form of auditing to ensure that all information transfers are authorized and that the parties are following the information security recommendations. Audits should include but are not limited to:

Action	Example
Assessment of potential security risks that pertain to the transfer of sensitive information.	Lack of oversight over how a group of consultants share information amongst themselves
Taking action to identify and patch these “weak spots”.	Put in place legal safeguards to ensure the consultants adhere to information security protocol.
Detecting potential cases of unauthorised disclosure.	Trace the transmission of a particular document containing sensitive information. Report incidents promptly to the sector leads and appropriate authorities.
Reinforcing safeguards in place.	Remind parties to adhere to information security principles and to follow SOP.

6.5 In conclusion, RPs must recognize the importance of information security for infrastructure security. These principles are strongly recommended for the RPs to follow and enforce when handling sensitive information to ensure that information concerning infrastructure security measures and vulnerability are kept guarded and thus remain effective against malicious actors.

REQUIREMENTS FOR PURPOSE-BUILT SHELTER REPORT

1 General Requirements

- 1.1 The Shelter Report shall document the performance-based design considerations for Purpose-built Shelters. This section describes the minimum level of protection, as well as other operational requirements for Critical Physical Infrastructures equipped with Purpose-built Shelters.
- 1.2 If the CPI only has a Workplace Shelter, a Shelter Report is not required.

2 Performance-Based Protective Designs

- 2.1 Purpose-built Shelters are designed for continued 24/7 operations throughout the high-risk period i.e., provide a safe area for personnel to work or rest without the burden of wearing the individual personnel protective equipment.
- 2.2 The Shelter Report shall be jointly prepared by the CP, architects, relevant Mechanical and Electrical (**M&E**) designers and consultants who are responsible for the planning, design, construction and commissioning of the Purpose-built Shelter. CPs, M&E designers and consultants are advised to follow the guidelines and parameters described herein so as to obtain the approval of Shelter Report from CPS.
- 2.3 The CP and M&E consultants can refer to Singapore Civil Defence Force's (**SCDF's**) Technical Requirements for S1-S5 or S10-S29 on details of Collective Protection (**COLPRO**) and shock protection systems. The Purpose-built Shelter design, including M&E designs, needs to be bespoke and performance based to meet RP's security objective.
- 2.4 The RP, CPs and relevant M&E designers and consultants are advised to follow the prevailing guidelines described herein and submit the Shelter Report during TVRA and SPP stages.
- 2.5 During the design phase, the RP should work closely with CP on ensuring a balanced trade-offs between project costs, systems serviceability/maintainability, and associated residual risks.

3 Submission Requirements

- 3.1 Before proceeding with the detailed design of a Purpose-built Shelter, CPs are advised to consult their RP on the management and operational aspects of the Purpose-built Shelter e.g., maximum occupants load, modes of operations, minimum period for continuous operation, etc.
- 3.2 CPs should prepare the Shelter Report that will comprehensively cover the following

areas:

- a. Introduction
- b. Design Basis Threats
- c. Purpose-built Shelter Design Considerations
 - i. General Planning Considerations
 - ii. COLPRO Designs
 - a) Main Entrance (with decontamination facilities)
 - b) Other Accesses (without decontamination facilities)
 - iii. Layout Planning for Purpose-built Shelter
 - a) Zones/Bounds of Protection
 - b) Door Types
 - i) Blast Doors and Gas-Tight Doors
 - ii) Gas-Tight Doors
 - c) Air Conditioning and Mechanical Ventilation (**ACMV**) components
 - i) Explosion Protection Valves (**EPV**)
 - ii) Overpressure explosion Protection Valves (**OBV**)
 - iii) Overpressure Valves (**OV**)
 - iv) Gas-tight Valves/Disk
 - iv. Air Shafts
 - v. Identification of critical assets (for Purpose-built Shelter)
 - vi. Design of Services
 - a) Electrical Supply system
 - b) Information Technology System
 - c) ACMV system. Ventilation, filtration and Purpose-built Shelter pressurisation requirements (boundary between 'clean' and 'dirty' areas to achieve gas-tightness, calculations on fresh air requirements, air flow / exchange rate, filtration system, details of protective valve system)
 - d) Water storage and distribution system
 - e) Sanitary and drainage system
 - vii. Structural Systems
 - viii. Shock protection design for services, equipment, architecture finishes and support structures.
 - ix. High-level commissioning test requirement for M&E system, COLPRO and other components to determine the functioning of the Purpose-built Shelter.
 - a) Air-Tightness Inspection
 - b) Internal Overpressure Test
 - c) Overpressure Regime & Airflow Test
 - d) Integrated Systems Test
- d. Residual Risks
 - i. Articulation of the likely residual risks
 - ii. Proposed contingency plans to reduce the risks, if applicable.

- e. Conclusion
- f. References



3.3 Relevant documents and drawings shall be attached in the Shelter Report for easy reference and a suggested list is shown in **Table A**.

Table A: List of information required in the Shelter Report

S/N	Description of Documents/Drawings
1	Structural layout plans showing the location of the Purpose-built Shelter, and the layout of the following items: <ul style="list-style-type: none"> a. Critical assets b. Bounds of protection and zoning of Purpose-built Shelter c. Separation chamber/blast lock and decontamination chamber d. Movement between the different shelter zones and levels e. Emergency infill points for power, water and electricity f. Sanitary and wastewater discharge points g. External structural hull members h. Details showing openings for service penetrations through walls and floor slabs
2	Areas of interdependencies and redundancies, such as external communication nodes, power supply system, chiller system, ventilation system, water supply system, gas filtration system and sewerage network (septic and wastewater), public address/intercom system, fire detection and sprinkler system, etc. Schematic drawings of the systems should demarcate the areas within the Purpose-built Shelter's bounds of protection.
3	<ul style="list-style-type: none"> a. Design summary for ACMV system, water supply system, and sanitary and drainage system b. Single line diagrams of the electrical installation in Purpose-built Shelter, communications systems c. Incoming electrical / telecoms / water routes to Purpose-built Shelter
4	Justification on the method of analysis, basis of computation and guidance on relevant standards as reference.
5	Elaboration of the adequacy of the COLPRO design against blast and Chemical and Biological and Radiological (CBR) threats, which include design of blast attenuation system, air side design guidelines, etc. for the survivability of people, and M&E systems; water pressure booster pump system, sanitary drainage/discharge system, wastewater drainage/discharge system.
6	Detailed calculations on: <ul style="list-style-type: none"> a. Air flow/exchange rate b. Purging dwell time within the air lock c. Details of protective valve system d. Air filtration system e. Overpressurisation regime for different zones f. Water demand and domestic water storage tank capacity g. Decontamination facilities, personal/mass decontamination water usage requirements, throughput time per cycle, etc.
7	In structure shock (ISS)/motion analysis on Purpose-built Shelter structural members (TM5-855-1). Results from the ISS analysis to be summarized and documented in the Shelter Report (using Table C in Annex D1).

8	Shock protection design, equipment fragility assessment (UFC 3-340-01) and summary of recommendations for essential/critical equipment and services.
10	Human throughput analysis of persons entering/exiting the Purpose-built Shelter, as well as movement between the different shelter zones and basement levels.
11	Provide details on the various modes of operation in Purpose-built Shelter i.e., ventilation mode, filtration mode and button up mode.
12	Provide details on security screening, Purpose-built Shelter's door monitoring system to detect abnormal changes in pressurization/COLPRO/M&E systems.
13	Proposed commissioning test(s) required for the certification of the equipment/installation required to determine the functioning of the Purpose-built Shelter, which can take reference from the Technical References for Public Shelters.

4 Testing and Commissioning (T&C) Requirements

- 4.1 The RP and CP shall work closely with the D&B contractor and Qualified Person(s) (**QP(s)**) to propose the method statements for tests and test reports for the commissioning of the Purpose-built Shelter. The commissioning requirements should be similar to the commissioning tests stipulated in BCA's commissioning requirements for public shelters.
- 4.2 Baseline commissioning testing requirements:
- a. Internal Overpressure Test to ensure that the external envelope of the Purpose-built Shelter guards against air leakage;
 - b. Overpressure Regime & Airflow Test to ensure that the air supply system can regulate airflow through the ducts, dampers and valves in accordance with the functions and requirements of the Purpose-built Shelter;
 - c. Integrated Systems Test to ensure that all systems in the Purpose-built Shelter continue to function properly and reliably under normal supply when switching to the standby generator set.
- 4.3 In addition to the commissioning tests above, the CP and QPs must also inspect and document the following test results at various stages of construction:
- a. Air-tightness inspection, Anchor bolts pull-out tests;
 - b. Individual function system tests;
 - c. Visual inspection of completed Purpose-built Shelter;
 - d. Purpose-built Shelter door tests;
 - e. Purpose-built Shelter shock tests.
- 4.4 All T&C reports should clearly state the design criteria stipulated in the Shelter Report, and be signed off by the RP before submission to CPS.

5 Certificate of Works Completion

- 5.1 The below documents are required to be submitted during CWC phase.
- a. Commissioning test reports and test records as mentioned in Para 4.1 and 4.2
 - b. Purpose-built Shelter conversion manual
 - c. Maintenance requirements
 - d. As-built drawings for Purpose-built Shelter components

6 References

- 6.1 Design, construction and commissioning of a Purpose-built Shelter shall take reference from the following documents⁴⁰ where appropriate:
- a. Civil Defence Materials & Workmanship (M&W) Specifications for S10-S29 Public Shelters;
 - b. Technical Requirements for S1 - S5 Public Shelters;
 - c. Technical Requirements for S10 - S29 Public Shelters;
 - d. Technical Specifications for Works of S1 - S5 Public Shelters;
 - e. Handbook for Commissioning Requirements of S1 - S5 Public Shelters⁴¹.
- 6.2 The RPs applying for approval of Purpose-built Shelter building, piling, structural, M&E plans shall ensure that their designs also comply with the latest editions of the relevant Codes of Practice, Acts, Regulations and statutory requirements of all other agencies who have jurisdiction over these requirements or systems.

⁴⁰ The Ministry Representative can contact SCDF_VCPD_Feedback@scdf.gov.sg to request for documents listed in Para 6.1 (a, b, c and d).

⁴¹ The Handbook for Commissioning Requirements of S1 - S5 Public Shelters is an online document that can be downloaded from BCA website