



GUIDE ON

OUTCOME-BASED SECURITY CONTRACTS

Second Edition
July 2022

Sector Lead:



**SINGAPORE
POLICE FORCE**
SAFEGUARDING EVERY DAY

Supported by:



SAS
SECURITY ASSOCIATION
SINGAPORE

Preface

The Security Industry Transformation Map (ITM) was launched in February 2018. The ITM's vision is to build a vibrant, technologically advanced, and competitive security industry that delivers enhanced security for Singapore and better jobs for Singaporeans. One key strategy to achieving this, is to transform the industry to rely less on manpower by leveraging technology. Since the launch of the ITM, the security industry has made progress on this front, with increasingly more outcome-based security contracts being implemented.

This Guide on Outcome-Based Security Contracts, first published in 2018, is a step towards achieving this vision. It aims to give service buyers step-by-step advice on how to write an outcome-based contract. This is important, because when buyers tender for services based on security outcomes rather than a fixed number of headcounts, security companies can innovate and deliver more productive solutions that integrate manpower, technology and processes. This can create better jobs, working conditions and employment terms for security officers. Service buyers also benefit from better value from higher quality services at lower long-term costs.

In this guide, you will find practical examples, clauses and templates that can be included in tender requirements. It also suggests performance management indicators to measure outcomes, and templates to evaluate proposals based on price and quality. The second edition of the guide also includes an alternative to assessing a contractor's performance, with the addition of the Demerit Points Model of assessment within the Performance Evaluation Matrix, as well as links to other useful resources relating to OBC.

With the implementation of the Security Agencies Competency Evaluation (SACE) since January 2022, service buyers can be assured that Security Agencies are assessed to be competent to perform security functions with a focus on providing technology-driven security solutions. The guide has also been updated to reflect the transition to SACE from the preceding Security Agencies Grading Exercise (SAGE). As we aim to regularly update this guide to keep it relevant, we welcome your feedback on the guide through MHA_Security_OBC_Helpdesk@mha.gov.sg.

The Security ITM Tripartite Committee thanks industry practitioners and tripartite stakeholders, who provided valuable suggestions as we developed this guide. We are confident that this guide will continue helping service buyers who are keen to switch to outcome-based contracting. Together, we can transform the security industry to keep Singapore safe and secure.

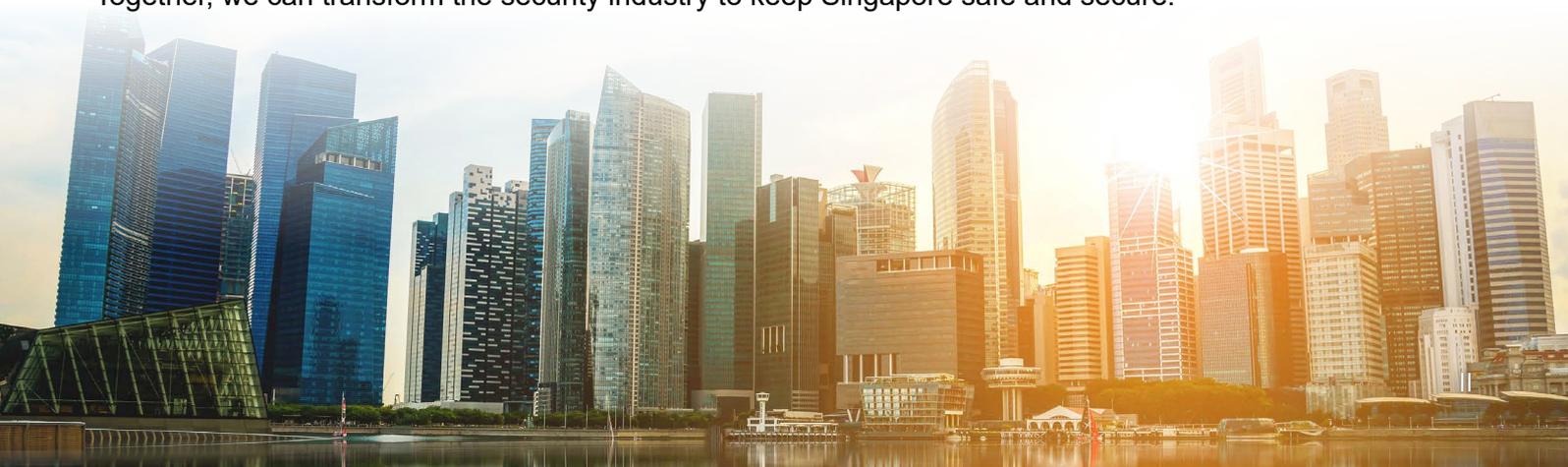


Table of Content

| | |
|---|----|
| 1. Introduction..... | 1 |
| 2. Features of Outcome-Based Security Contracts..... | 2 |
| 3. Guidelines for Drafting OBC..... | 4 |
| 3.1 Pre-Tender Stage..... | 4 |
| 3.2 Tender-Drafting Stage..... | 6 |
| 3.2.1 Tender Instructions..... | 7 |
| 3.2.2 Scope of Work..... | 10 |
| 3.2.3 Performance management..... | 14 |
| 3.2.4 Pricing Model..... | 17 |
| 3.3 Tender-Evaluation Stage..... | 18 |
| 3.3.1 Ensure a Holistic Evaluation..... | 18 |
| 3.3.2 Using Price-Quality Method (PQM) as the Evaluation Framework .. | 19 |
| 4. Examples..... | 23 |
| 4.1 List of Tender Instructions for Security OBC..... | 23 |
| 4.2 Sample Scope of Work for Security OBC..... | 30 |
| 4.3 Monthly Performance Evaluation Matrix..... | 43 |
| 4.4 Demerit Points Model..... | 46 |
| 4.5 Tender Evaluation..... | 49 |
| 5. List of Resources..... | 53 |

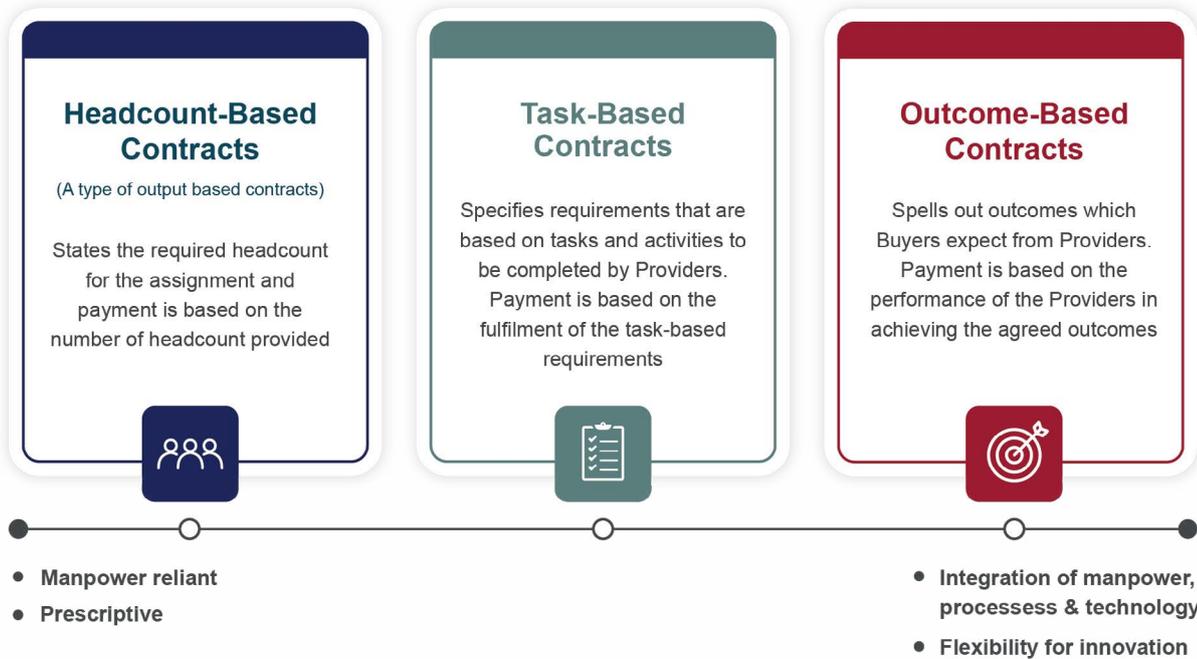
Section 1:

Introduction

Outcome-Based Contracting (OBC) refers to service buyers specifying contract requirements in terms of expected performance levels, rather than output levels. In contrast, traditional output-based contracts specify fixed amounts of resources (e.g. manpower, equipment) that the service provider needs to supply.

OBC can lead to better solutions compared to output-based contracts. OBC allows providers to propose innovative security solutions that use less resources to meet desired security outcomes, by taking advantage of technology and re-designing of work processes. OBC can improve cost-effectiveness and reduce manpower reliance. OBC does not preclude manpower requirements. Instead, it seeks to integrate manpower, technology and processes, making it more sustainable for buyers in the long term, given rising manpower costs.

This guide applies to security services to protect buildings and premises. It provides buyers with guidelines and templates on how to adopt OBC, from planning a tender to evaluating bids. Buyers can adapt the guidelines and templates for their own requirements.



Section 2:

Features of Outcome-Based Security Contracts



The key features of outcome-based contracts for security services are:

a) Outcome-Based Specifications

Outcome-based specifications describe security outcomes, operational parameters and performance demands instead of just specifying output (e.g. headcount). This gives providers the flexibility to offer the most effective solution by integrating manpower, technology and operational processes.

Refer to Section 3 on best practices to develop an outcome-based scope of work and Section 4.2 for a sample scope of work for security outcome-based contracts.

b) Outcome-Driven Performance

The performance of the providers shall be tracked against desired security outcomes. A performance management matrix or demerit points model can be utilised and should include both quantitative and qualitative metrics to assess the performance of the providers. Buyers will need to formulate metrics that best meet their requirements in the outcome-based specifications.

Refer to Section 3 on best practices to implement outcome-driven performance management and Section 4.3 for a sample performance evaluation matrix and Section 4.4 for a demerit points model.

c) Quality-Focused Evaluation

Quality attributes should take on heavier weighting compared to price during evaluation of an outcome-based contract. The emphasis on quality benefits providers who provide clear and convincing explanations of how their proposal will achieve the desired outcomes.

Refer to Section 3 on best practices to adopt during OBC evaluation and Section 4.5 for a sample of tender evaluation report.

d) Productivity Enhancement Framework

Continual process enhancements should be part of OBC. As providers understand operations better over time, they should be incentivised to propose changes which are able to achieve the same security outcomes at lower cost and with more efficient use of resources. That said, it is essential that providers understand that their responsibilities and contractual service levels must be maintained when any such proposal is implemented.

Refer to Section 3 on best practices to enhance productivity in OBC and Section 4.2 for a sample scope of work for security outcome-based contracts.

e) Adaptive Pricing to Regular Contract Reviews

Outcome-based contracts must have flexibility to adapt to changing market conditions and government regulations. By doing so, it allows risk to be shared between buyers and providers in a fair and open manner. However, in cases where inflation-driven cost adjustment formulas are applied, buyers should take into account the wage requirements under the Progressive Wage Model¹ (PWM), when considering any downward price adjustments (e.g. due to negative economic conditions).

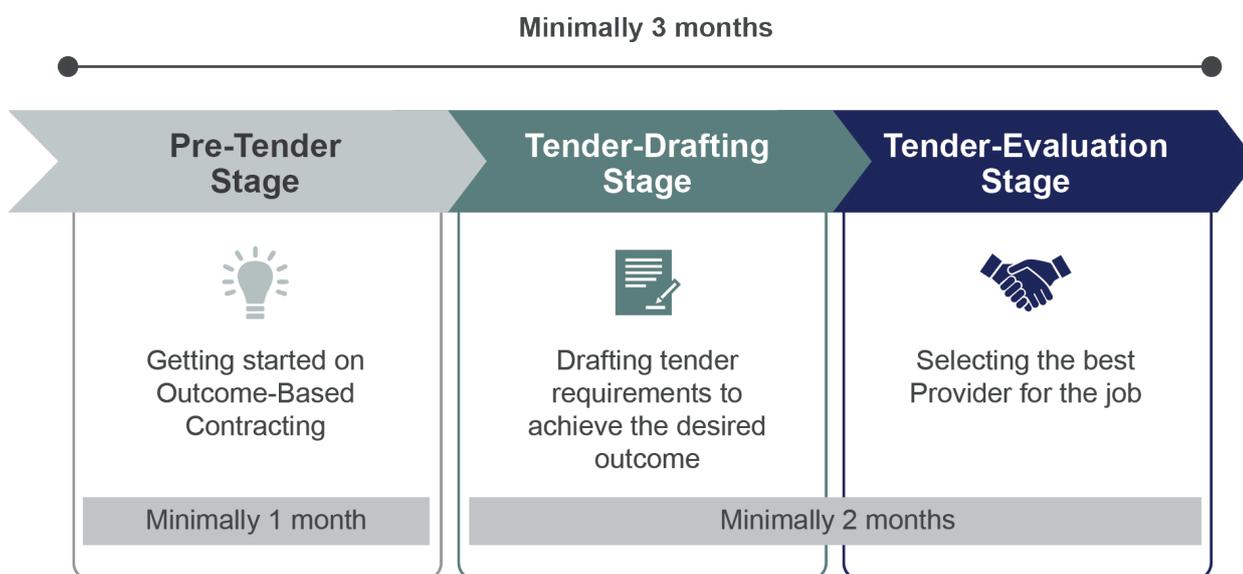
Refer to Section 3 on best practices for adaptive pricing and Section 4.2 for a sample scope of work for security outcome-based contracts.

¹ For more information on the PWM, readers may also refer to other security industry-related documents under the Security Tripartite Cluster section found on www.ntuc.org.sg/tripartiteguidelines.

Section 3:

Guidelines for Drafting OBC

The security service procurement process typically consists of three stages. Buyers should set reasonable timelines for each stage- pre-tender, tender drafting and tender evaluation. As a general rule, at least three months should be set aside. This section details the process and best practices for the different phases.



3.1 Pre-Tender Stage

Getting started on OBC

Planning for procurement should be conducted as early as possible. This is when there is the greatest potential to propose significant ways to enhance security and improve productivity.

a) Enhancing Security Operations Upstream

At the strategic level, buyers should review opportunities to enhance security operations and derive productivity savings through infrastructure development and demand aggregation. When new infrastructure is built or existing infrastructure retrofitted, buyers can incorporate security

procedures, physical protection concepts and security technology into the building's security design and plans². Clustering security demand can also often achieve better synergies in operations and resource efficiency. Clustering can be done geographically (i.e. multiple sites within the same geographical location) or within an organisation (i.e. different sites within the same organisation). Clustering needs to be done with awareness of contracting timelines and provisions to allow smooth on-boarding of the various sites. This should be planned at least a year before the tender is called.

b) Security Risk Assessment

It is important for buyers to be able to define security outcomes and understand how security outcomes are being met when a proposal is put forth in OBC. Security risk assessments will provide buyers with an evaluation of security risks in a given operating site through analysis of threats, vulnerability and consequences. At least 3 months should be set aside if buyers are undertaking a comprehensive security assessment outside of the Tender. For such comprehensive security assessments, buyers may engage an accredited security consultant³ to assist in crafting their outcome-based contracts at the pre-tender stage. For integrated/ basic security contracts, the security risk assessment can be conducted as part of the tender exercise.

c) Market Surveys and Pre-Qualification of Providers

Buyers should assess potential providers to determine their suitability to participate in the tender, through a market survey or a Request for Information (RFI). Buyers should set aside at least one month for this process, which will involve discussions with potential providers. Buyers can consider pre-qualifying providers and invite them to bid for the tender.

² Readers can also refer to the *Guidelines for Enhancing Building Security in Singapore* found on <https://www.police.gov.sg/Advisories/Infrastructure-Protection/Building-Security>

³ A list of industry-accredited security consultants can be found on <https://scap.info>



3.2 Tender-Drafting Stage

Incorporating Outcome-Based Requirements in Tender Documents

Buyers should incorporate outcome-based requirements into tender documents that clearly communicate the expectations and standards expected from the providers. The table below summarises the suggested best practices during tender drafting.

| Section | Practices |
|-------------------------------------|---|
| 3.2.1 Tender Instructions | <ul style="list-style-type: none"> a. Security risk assessment b. Operational model c. Resource plan d. Transition plan e. Price schedule f. Licensing and competencies g. Company profile and experience h. Evaluation criteria i. Clarifications |
| 3.2.2 Scope of Work | <ul style="list-style-type: none"> a. Contract duration b. Area of coverage c. Operational hours d. Security outcomes e. Other services f. Surges and contingencies g. Additional obligations |
| 3.2.3 Performance management | <ul style="list-style-type: none"> a. Performance metrics b. Performance evaluation matrix/ Demerit points model c. Incentives for good performance d. Service failure |
| 3.2.4 Pricing Model | <ul style="list-style-type: none"> a. Fixed pricing model <u>OR</u> b. Price review model |

3.2.1 Tender Instructions

Tender instructions refer to instructions to guide providers in the submission of information needed for evaluation. Instructions should be clearly laid out and templates given whenever possible. There are nine broad categories of information that buyers should include in an OBC tender instruction.

a) Security Risk Assessment

A security risk assessment needs to be done prior to contracting. Buyers can consider two ways of building this into their procurement process:

(i) **Separate/Comprehensive.** This is a security assessment that is done separately and before the tender for security services is called. It is a comprehensive assessment of the infrastructure plans and operations, done by external or in-house security consultants. The consultants will propose desired security outcomes with a corresponding security technology and operating concept plan. Deliverables could include draft tender specifications which the buyer can use. As this assessment takes time and is costlier, it is recommended mainly for buyers who have complex, high-security or multiple premises to secure.

(ii) **Integrated/Basic.** This is a condensed security assessment which is integrated into the tender process. It is best suited for buyers who have smaller premises where such an assessment can be conducted by security service providers as part of developing their tender bids. This security assessment should provide the rationale and planning parameters for proposed solutions, and how the solutions will meet the identified security outcomes.

b) Operational Model

Buyers should request providers to submit a detailed proposal on their operational model. The proposal should explain how the manpower, processes, infrastructure and technology will be integrated effectively to mitigate security risks identified by the security risk assessment as well as performance demands specified in the tender documents.



c) Resource Plan

Buyers should encourage providers to adopt technology and work process that can maximise efficiency of their manpower to meet the stipulated security outcomes. Should buyers require providers to use equipment that are owned by the buyers, the list of equipment should be provided in the tender documents. Buyers could also specify in the tender documents, any operating systems or technology that they want the providers to use. Buyers may refer to the Security Industry Digital Plan (<https://www.imda.gov.sg/programme-listing/smes-go-digital/industry-digital-plans/security-idp>) to consider suitable technology solutions, for inclusion into their requirements.⁴ Buyers should assess the providers' submitted list of equipment, materials, schedule of work and deployment proposal/plan for their suitability and effectiveness.

d) Transition Plan

Buyers should request providers to submit a transition plan to show the timeline for operations to ramp up to full operational capability under the proposed operating model. The plan should provide explanations on how change management and technology deployments would be performed (if applicable) and what measures would be implemented if transition plans go beyond the buyers' stated deployment timelines. Information on existing security systems can be made known to the tenderers for them to consider the usefulness and possible integration as part of the offered solution. Buyers could also seek the new service provider's assistance to aid in the transition process such as handing/taking over of existing systems from the outgoing service provider.

Note

Technology and infrastructural changes may require a transitional period before full operational capability is achieved. The Tenderer must make transition periods clear and explain how interim operations would be supported.



e) Price Schedule

Buyers should define the baseline and ad-hoc or surge service items for price submissions. This would form the basis for price assessment during the tender evaluation stage. Ad-hoc or surge services should be offered as separate scheduled rates as the frequency of recurrence is unknown. This removes the need for providers to cater for capacity buffers in the price submission. Otherwise, buyers will end up bearing the costs for provisions that are not utilised.

⁴ The Security Industry Digital Plan was jointly developed by the MHA, the Infocomm Media Development Authority (IMDA), and the industry, to provide a step-by-step guide on the digital solutions local SMEs in the security industry can adopt at each stage of their growth.

Service buyers would need to forecast possible events that may require the deployment of additional manpower. This would be considered an ad-hoc demand and should be incorporated into the tender. Tenderers can then propose the rates for additional manpower required for these events.

f) Licensing and Competencies

Security agencies (SAs) must possess a valid licence, throughout the duration of the Contract. SAs which fail the Security Agencies Competency Evaluation (SACE)⁵ assessment will not be issued with a valid licence and would be given 2 months grace period to cease operations and hand over their current contracts.

g) Company Profile and Experience

Buyers can also request for additional information related to the company profile and experience which could be factored into evaluation. This should be worked out concurrently with the development of the evaluation criteria and their parameters.

h) Evaluation Criteria

Buyers should communicate the evaluation criteria for the tender in the tender documents. This offers transparency in the evaluation of submitted proposals and will help providers in proposing the appropriate operational model and resources to meet the security outcomes.

i) Clarifications

Buyers should include contact details of the procurement officers should providers require further clarifications on the tender requirements and submission.

⁵ The SACE framework assesses SAs on how much they harness technology to augment critical areas such as training, operations, command, control and communications. With SACE, service buyers can be assured that SAs have been assessed to be competent in critical areas. In 2023, elective competencies will also be introduced to SACE, allowing service buyers to identify SAs with the capabilities to meet their specific needs. More information on SACE can be found on <https://www.police.gov.sg/e-Services/Police-Licences/Security-Agencies-Competency-Evaluation>

3.2.2 Scope of Work

This section states the key elements to be specified by the buyers in order for the providers to plan and prepare the proposal for the required security services.



a) Contract Duration

Definition of the firm and optional contract period. Establishing longer contract durations would translate to stable services and lower amortised cost for use of technology solutions. Longer contract duration also helps providers to retain talent who are familiar with the job requirements and working environment, allows providers to invest in training, and provides a longer cost recovery period for technology investment. As a guide, buyers can consider a contract period of at least three years. Buyers can extend this to cover the nature of contract extension (e.g. lead time to notify contract extensions) and how it will affect pricing components (e.g. schedule rates and optional services).

Recommended contract duration

- (i) Contract with less than S\$1M estimated annual contract value should have a minimum of a three-year firm contract period.
- (ii) Contract with more than S\$1M estimated annual contract value should have a minimum of a five-year firm contract period, or three-year firm contract period with two-year option period.

b) Area of Coverage

Definition of the area of deployment which falls under the scope of the contract. It can include projections of peak or low activity volume at different locations. Sensitive or inaccessible areas which require increased surveillance or higher security classification should be flagged out in the requirements.

c) Operational Hours

Definition of the deployment hours which services are to be rendered or any specific schedules that affect operational activities on the ground.

d) Security Outcomes

Definition of the type of security services to be rendered, the operating parameters which needs to be considered, with corresponding explanations and performance measurements on the outcomes to be achieved. Security outcomes are major factors which affects how operations will be run and will be the reference point in deciding if services provided were adequate. Security outcomes should be defined by buyers based on an understanding of what the existing operations can achieve and whether there is a need to impose more stringent demands. Overly stringent demands can drive up costs unnecessarily. Service level requirements set should also be reasonable and achievable by the providers. The table below illustrates sample outcome-based statements based on desired outcomes that buyers can adapt for use when drafting tender requirements.

| Desired Outcome | Examples of Outcome-Based Statements |
|---|--|
| Protection of occupants and property | All visitors must be registered in the Visitor Management System and issued visitor passes |
| | No incidents relating to loss or damage of property |
| | All intrusions are detected, recorded and correct response rendered |
| Security with minimal service failure and timely service recovery | Ensure 80% of visitors with registration waiting time < five minutes |
| | Achieve overall customer satisfaction of security services of at least 80% |
| | CCTV systems provided has system availability of > 95%, failures are rectified within two hours |
| | Ensure number of complaints per month is less than five |
| Sense of security and visible presence | Ensure all scheduled patrols were conducted [Note: Physical patrols may be replaced by virtual patrolling.] |
| | Ensure 90% attendance of SOs |
| | Ensure number of incidents where SOs fail to respond within 15 minutes is less than five per month |

e) Other services

Defining other secondary duties or supplementary tasks that providers are obligated to perform as part of security duties. (e.g. provide help desk services to direct visitors). Such tasking should be kept minimal to allow providers to focus on security operations and buyers should only include work functions that complement security operations. For non-security related functions (e.g. landscape management), buyers should specify that providers can provide non-security-trained staff to undertake these functions.

Note

As part of fair contracting terms, buyers should be clear that services not included in the scope of work but are requested during the contract period shall be considered additional services for which fair remuneration should be provided. If this principle is adhered to, service offers from providers will not have to factor in buffers for unknown needs which can unnecessarily increase prices.



f) Surges

Defining how surges would be handled and how fast providers will need to respond if surge demands are encountered. As a norm, surge demand should not be factored into routine needs and should be included as additional scope of work.

Example of possible demand surges:

Hosting of events on site, heightened security alerts etc.

(i) Known surges

Buyers could define such surges and what is expected from the providers when it occurs. If requested as a Tender submission request, providers can be requested to submit a proposal of their response plans and price package for every activation of such surge demand.

(ii) Unknown surges

Surge demand provisions can be worked out with the provider whenever the buyer identifies a need during the contract period. This gives buyers the assurance that surge demands can be met.

g) Additional Obligations

These are broad demands that buyers may include as areas which providers have to abide with such as:

- Training and competency demands
- Code of conduct
- Conduct of audits and reviews
- Safety management and liability
- Security screening of providers' officers
- Supply of providers' furnished equipment and their specifications
- Use and maintenance of buyers' security equipment
- Contractual review points and price review mechanisms
- Productivity enhancement frameworks
- Obligation for periodic contract demand reviews
- Tripartite Guidelines on Fair Employment Practices (TGFEF)



3.2.3 Performance management

To encourage providers to deliver good service, buyers can tie performance indicators to desired outcomes. One practical model is the use of performance-based payments to reward providers who have performed well based on the service-level requirements. It should not be used to penalise providers to lower contract costs. Should buyers decide to adopt a performance-based payment model, the following information on how payment is pegged to the performance scores should be included in the tender documents:



a) Performance Metrics

It is important for buyers to determine clear, measurable performance metrics (both quantitative and qualitative) that are linked to security outcomes in the tender documents for subsequent evaluation of contractual performance. How performance data will be collected and calculated to evaluate performance must be clearly defined.

b) Performance Evaluation Matrix / Demerit Points Model

Buyers should track the performance of the providers' performance based on a performance evaluation matrix/demerit points model. The performance matrix/demerit points model should clearly reflect all the metrics that will be used to assess the performance of the service provider.

Refer to Sections 4.3 for a sample performance evaluation matrix and 4.4 for a sample demerit points model respectively



c) Incentives for Good Performance

In order to encourage providers to meet or exceed performance standards on a regular basis, buyers are encouraged to adopt some form of reward system to incentivise providers. Buyers may choose to adopt either the non-monetary reward system, or the incentive payment model or both. Service buyers can take such incentives into consideration when budgeting.

Example of incentives:

(i) Monetary Rewards (Recommended)

Monetary rewards can be in the form of a percentage of payment sums issued at periodic intervals to providers. It is important to state that such rewards are to be shared between providers and their officers, to incentivise officers to play a proactive role in meeting the outcomes. A general guide would be 30% to providers and 70% to their officers, coupled with provisions for buyers to validate that this was apportioned fairly.

(ii) Non-monetary Rewards

This can be in form of periodic appreciation events or gifts for individual officers. Buyers can also leave it to providers to propose a reward system.

d) Security Failures

Owing to the nature of security services, it is not practical to manage all security failures using performance indicators. Failures of these nature will have to be dealt with whenever they are detected. To discourage occurrences of security failures, contractual tools (e.g. warning letters, payment mechanisms, disqualification from contract option extension, or termination) could be applied. Monetary disincentives should always be reasonable and proportional with the nature of the failure, and buyers should be mindful that unreasonable pricing may affect financial positions of providers and the ability to pay their workers. Contract termination should apply in cases where persistent failures continues and there is clear evidence that the provider is not capable of delivering contracted outcomes. If the contract is terminated, a reasonable time frame should be considered and reasons for the termination be made known to the provider.

Example: Performance-Based Payment Model

Buyers should specify the payment model detailing the frequency of performance evaluation and minimum score to be attained for the corresponding payment amount. The payment amount which is to be applied can vary and should be decided by the buyers depending on the criticality and impact of security lapses to operations. Providers can then price in their risk provisions accordingly.

For example, when the buyer sets a minimum total score of 24 per month, the provider will receive full payment when a minimum baseline score of 24 (i.e. total score across six indicators) is achieved for the month.

Sample Payment Model

| Score | Monthly Payments |
|--------------------------------|------------------|
| 27 (Bonus) | 105% |
| 24 – 26 (Baseline) | 100% |
| 10 - 23 (Below Average) | 95% |
| <10 (Poor or Security Failure) | 90% |

In this example, when the buyer set an incentive payment of 105% payment, assuming each indicator has maximum score of four for meeting baseline expectation and one bonus point when performance exceeds expectations. Provider will need to exceed performance in three out of six indicators in order to reach a total score of 27.

Conversely, to discourage poor performance / security failure, buyers can tier payment according to the set payment model.

If contract termination in the event of repeated poor performance or repeated security failures is to be applied, the grounds for termination must be clearly stated. Buyers should also allow adequate notice periods and provide clear transitional plans.

In addition to the above, buyers may wish to include a clause to preserve the usual rights of parties at law that can be exercised in addition to the contractual rights.

3.2.4 Pricing Model

Buyers can choose to adopt a Fixed Price Model or Price Review Model for the contract. Although a Price Review Model is more complex, it is useful for longer-term contracts as it allows even sharing of pricing risk, which could be unknown at the point of contracting. It also avoids situations where providers are forced into unsustainable operations due to external conditions. As part of fair contracting terms, buyers may also include terms that allows reasonable changes in prices if providers are able to provide justifications on basis of unforeseeable circumstances (e.g. force majeure events) that can lead to higher operating costs during the contract period.

Pricing Models:

(i) Fixed Pricing Model

Contractual rates remain constant throughout the contract period; any changes will be subject to mutual agreements via contract variations.

(ii) Price Review Model

Baseline rate is established for a defined period coupled with established means of reviewing the prices to account for external price changes. Provisions for pricing reviews could include one or more of the following:

- Fixed percentage price escalation which can be proposed by provider or defined by buyer. Price escalation would generally apply to material and manpower provisions being contracted. Provider may factor in escalation on their overheads as well since cost for these components would grow with time.
- Cost adjustment factors using formulas that take into account different economic indices.
- Obligations to review pricing in event of government policy changes which has cost impact on resources (e.g. PWM), or other economic forces such as inflation.
- Obligations to co-share savings in the event provider is able to receive technology or productivity grants or subsidies from government for contracted operations.

Note:

Contractual price reviews can be complex if pre-agreed principles are not established in contract. As part of fair contractual terms, contracts should include clauses that allows both parties to call for a termination of contract in accordance with mutually agreed notice periods. If necessary, termination may be restricted to specified conditions for both parties.



3.3 Tender-Evaluation Stage

Selecting the Best Provider for the Job

After the tender has closed, buyers should conduct a tender evaluation in an organised manner based on pre-determined quality criteria, weighted against pricing. Beyond evaluation to select recommended offers, buyers should also assess the sustainability of offered prices from the selected tenderer. The table below summarises the steps which buyers can take to evaluate and select the best provider for the job.

| Section | Practices |
|---|---|
| 3.3.1 Ensure a holistic evaluation | <ul style="list-style-type: none">a. Cardinal requirementsb. Evaluation parametersc. Tender interviews and reference checks |
| 3.3.2 Using Price-Quality Method (PQM) as the evaluation framework | <ul style="list-style-type: none">a. Determine the weightings for Price and Quality criteriab. Set up the scoring system for Pricec. Set up the scoring system for Qualityd. Aggregating the P-Score and Q-Score |

3.3.1 Ensure a Holistic Evaluation

Cardinal requirements and evaluation criteria should be clearly marked out in the tender documents. In addition to the procurement officers, relevant personnel who will oversee the providers should be invited to sit in the Tender Evaluation Committee (TEC). Communicating the evaluation criteria to the TEC early during the tender stage will help align their expectations with the outcome of the security contract.

a) Cardinal Requirements

These are requirements specified by the buyers in the tender instructions which are mandatory for providers to fulfil as part of tender submission. Upon receipt of the tender proposals, the TEC should review submissions to determine if the proposals have met the cardinal requirements. Any offers not in compliance should be deemed invalid and excluded from evaluation.

Refer to Section 4.1 for a sample list of tender instructions for security OBC.

b) Evaluation Parameters

Buyers should communicate the evaluation criteria for the tender in the tender documents to help providers better understand the requirements and propose the operational model and resources that best meet the security outcomes. The evaluation parameters would also serve as guidelines to help the TEC score each criterion. Buyers can consider using the Price-Quality Method (PQM) as the evaluation framework.

c) Tender Interviews and Reference Checks

Buyers can also arrange interview sessions with shortlisted providers after the tender has closed. These sessions allow buyers to better understand the value proposition offered by the providers and clarify on the different proposals submitted. Buyers can also conduct reference checks through telephone calls / site visits to existing or past clients to assess the quality of service provided by the providers.

3.3.2 Using Price-Quality Method (PQM) as the Evaluation Framework

The Price-Quality Method (PQM) is an established evaluation methodology that allows for fair and balance evaluation of tender proposals. When adopting the PQM in tender evaluation, buyers should evaluate the submitted proposals using pre-agreed definition on the following:

a) Weightings

There are two components in the PQM approach – Price and Quality. Both components are assigned weightings and overall score computed. The contract would be awarded to the tenderer with the highest overall score. In evaluating outcome-based contracts, buyers should generally aim towards a 40:60 weighting between Price and Quality. The weightings may be adjusted according to the needs of the buyers.

b) Scoring System for Price

Buyers can work out the P-Score to compare the cost effectiveness of the tender proposals. The formula to use in calculating the P-Score would be: $\text{Lowest Tenderer Proposal cost} / \text{Tenderer's offered Proposal cost}] \times \text{Price Weighting}$ (set at 40%, for example). Buyers should consider the total cost of contracted services over the contract period and factor in cost of surge demands by using projections of usage if necessary. Buyer should also further check on the sustainability of

the offered prices. If offered prices are unnaturally low, it can mean that the tenderer may not be able to operate sustainably throughout the contract period. For example, if a tenderer's offered price is only S\$20,000 per month when the buyer's assessment is S\$80,000 for the proposed manpower, cost of technology and infrastructural build-up, this could lead to unsustainable operations downstream. Buyer should undertake further clarifications with the tenderer and assess if this is an acceptable contracting risk.

c) Scoring System for Quality

In determining the scoring system for quality, buyers will need to first determine the quality-related criteria and distribution points, before coming up with a rating system for each evaluation criterion. Buyers can adopt the following steps in determining the scoring system for quality.

Step 1: Determine quality-related criteria and distribution points

Quality-related criteria refer to the different components to be evaluated to ascertain the quality of the submitted proposals. Each criterion should be assigned points according to their relative importance. For example, if the focus of the OBC is to leverage technology and minimise manpower reliance, a greater weighting should be given to quality of technology solutions.

| Quality Criteria | Weighting |
|--|-----------|
| Quality of technology solutions | 30% |
| Quality of proposed security solutions | 70% |

Quality evaluation can include other quality criteria (e.g. training systems, human resource (HR) practices, track records, etc.)

Step 2: Determine rating system

The TEC will then score each criterion using an agreed rating system. For example, the rating system for both quality criteria could be:

| Point | Description |
|-------|--|
| 0 | Proposed solution will achieve security outcomes which are worse-off than current operations |
| 1 | Proposed solution will achieve security outcomes similar to current operations |
| 2 | Proposed solution will achieve better security outcomes in at least 1 area |
| 3 | Proposed solution will achieve better security outcomes in more than 1 area |

d) Aggregating the P-Score and Q-Score

Buyers can adopt the following steps to evaluate tender proposals using PQM (40% for Price and 60% for Quality, for example):

Step 3: Calculate the P-Score

Based on three tender proposals submitted where Tenderer C has the lowest offered price, the P-Score for the three tender proposals can be worked out below:

| | Tenderer A | Tenderer B | Tenderer C |
|------------------------|-------------|-------------|-------------|
| Price Submitted | \$1,100,000 | \$900,000 | \$750,000 |
| Lowest Price Submitted | \$750,000 | \$750,000 | \$750,000 |
| Weighting | 40% | 40% | 40% |
| P-Score* | 0.27 | 0.33 | 0.40 |

* P-Score = [Lowest Tenderer Proposal cost / Tenderer's offered Proposal cost] x Price Weighting

Step 4: Calculate the Q-Score

Q-Points can be calculated based on the weighting assigned to the quality criteria. An individual Q-Score can be calculated to compare the quality of the proposals amongst the three tenderers.

For example, Tenderer A has achieved the highest Q-Points of three points and based on a Price: Quality weighting of 40:60, the Q-Score of the three Tenderers can be derived below.

| Criteria | Tenderer A | | Tenderer B | | Tenderer C | |
|--|-------------|-----------|-------------|------------|-------------|------------|
| | Score* | Q-Points† | Score | Q-Points | Score | Q-Points |
| Quality of technologies solutions (30%) | 3 | 0.9 | 3 | 0.9 | 1 | 0.3 |
| Quality of proposed security solutions (70%) | 3 | 2.1 | 1 | 0.7 | 2 | 1.4 |
| Total | 6 | 3 | 4 | 1.6 | 3 | 1.7 |
| Q-Score‡ | 0.60 | | 0.32 | | 0.34 | |

* Scores represent actual scoring awarded to Tenderer for that Quality criteria

† Q-points = [Score x Weightings]

‡ Q-Score = [Tenderer Total Q-point / Highest Total Q-point amongst Tenderers] x Quality Weighting (set at 60%)

Step 5: Aggregating the P-Score & Q-Score

The total combined score calculated based on the price and quality assessment of the three proposals can be worked out below. Tenderer A scored the highest and should be recommended for award.

| | Tenderer A | Tenderer B | Tenderer C |
|---------------------|-------------------|-------------------|-------------------|
| P-Score | 0.27 | 0.33 | 0.40 |
| Q-Score | 0.60 | 0.32 | 0.34 |
| Total Score* | 0.87 | 0.65 | 0.74 |

* Total Score = P-Score + Q-Score

Refer to Section 4.5 for a sample tender evaluation report.



Section 4: Examples

4.1 List of Tender Instructions for Security OBC

This section outlines a list of examples of Tender Instructions that can be adapted into buyer's tender documents. Buyers should adapt the examples according to their unique requirements when drafting Tender Instructions.

| Items to include | Examples of Tender Instructions |
|-----------------------------|--|
| General instructions | <p><Name of buyer> wishes to engage a security provider (hereafter known as "tenderer") to provide security services for the company's premises.</p> <p>All interested tenderers must attend a Tender Briefing and Site Visit on <Date, Time, Venue>.</p> <p>Tenderers are requested to develop proposals based on a security risk assessment of buyer's site, security outcomes and operational parameters stated in the tender documents. Each Tender Offer must be submitted with the following contents:</p> |
| a) Security Risk Assessment | <p>Tenderer must submit an analysis of security risk and operational considerations in relation to the Tender Specifications and site surveys.</p> <p>Note: This is to be submitted in the form of a TVRA table covering Threat Description, Probability, Severity Level, Risk Level, Control Measures proposed in Tender, and Residual Risk Level.</p> |

| Items to include | Examples of Tender Instructions |
|--|---|
| <p>b) Operational Model</p> | <p>Tenderer is required to study the site and <u>submit</u> a proposal for the operational model covering how manpower, processes, infrastructural and technology will be integrated to meet the security outcomes.</p> <p>Tenderer should explain why the proposed model is adequate in relation to the observations made in Security Risk Assessment and the security outcomes defined. Tenderer should also highlight proposals that are able to achieve security outcomes beyond the ones defined in Tender.</p> <p>If technology solutions are suggested, tenderers should provide the committed availability levels and explain the Business Continuity Plans when software or equipment fails.</p> <p>The objective of OBC is to ultimately ensure better security outcomes. With OBC, when a risk assessment is done, risks identified can be addressed through the implementation of appropriate measures.</p>  |
| <p>c) Resource Plan</p> | <p>Tenderer shall <u>submit</u> a resource plan covering the necessary and appropriate resources (equipment, manpower, tools) to perform the required services and enhance productivity and service performance.</p> <p>Tenderer must submit a resource plan listing out the optimum manpower structure, equipment and technologies that will be committed to the operations. Details must be provided to explain why the proposed resources are adequate to support the services.</p> |
| <p>d) Transition / Implementation Plan</p> | <p>Tenderer is to <u>submit</u> a transition plan illustrating how services and technology will be implemented during transition. The plan shall include clear timeline and milestone of key activities when taking over. Tenderer should specify additional time required for implementation and testing of technology, equipment, processes or infrastructures during the transition, together with what the tenderer will be provisioned to do during the interim period.</p> |

| Items to include | Examples of Tender Instructions | | | | | | | | | | | | | | | | | | | | | | | | |
|--|---|---------------------|---------------------|------------------|-------------|------------------|--|--|--------|--------|--------|--------|--------|--------------|---------------------|---------------------|---------------------|-------------|-------------|-------------|---------------------|---------------------|---------------------|-------------|-------------|
| d) Transition / Implementation Plan (continue) | Any existing security systems can be made known to the tenderers for them to consider the possibility of integration with their offered solutions. Service buyers could also seek the new service provider's assistance to aid in the transition process such as handing/taking over of existing systems from the outgoing service provider. | | | | | | | | | | | | | | | | | | | | | | | | |
| e) Price Schedule | <p>Tenderer is to <u>submit</u> comprehensive rates in the format provided in the following tables. The monthly rate quoted should include proposed manpower, process reviews, trials, infrastructural changes and use of technology during the contract period.</p> <table border="1" data-bbox="416 624 2051 903"> <thead> <tr> <th data-bbox="416 624 703 675">Contract Period</th> <th colspan="3" data-bbox="703 624 1514 675">Firm Period</th> <th colspan="2" data-bbox="1514 624 2051 675">Optional Period*</th> </tr> <tr> <th data-bbox="416 675 703 726"></th> <th data-bbox="703 675 972 726">Year 1</th> <th data-bbox="972 675 1240 726">Year 2</th> <th data-bbox="1240 675 1514 726">Year 3</th> <th data-bbox="1514 675 1783 726">Year 4</th> <th data-bbox="1783 675 2051 726">Year 5</th> </tr> </thead> <tbody> <tr> <td data-bbox="416 726 703 815">Monthly rate</td> <td data-bbox="703 726 972 815">Tenderer to propose</td> <td data-bbox="972 726 1240 815">Tenderer to propose</td> <td data-bbox="1240 726 1514 815">Tenderer to propose</td> <td data-bbox="1514 726 1783 815">Upon review</td> <td data-bbox="1783 726 2051 815">Upon review</td> </tr> <tr> <td data-bbox="416 815 703 903">Annual cost</td> <td data-bbox="703 815 972 903">Tenderer to propose</td> <td data-bbox="972 815 1240 903">Tenderer to propose</td> <td data-bbox="1240 815 1514 903">Tenderer to propose</td> <td data-bbox="1514 815 1783 903">Upon review</td> <td data-bbox="1783 815 2051 903">Upon review</td> </tr> </tbody> </table> <p data-bbox="416 954 2051 1070">* Year 4 and 5 rates are to be established on Year 3 based on average of Total Wage change (%) from Year 1 and 2 reported in Report on Wages in Singapore published by the Manpower Research and Statistics Department, Ministry of Manpower, Republic of Singapore. See example below:</p> <p data-bbox="416 1123 2051 1240">If Year 1 = 1.5% and Year 2 = 5%, the average Total Wage Change (%) = 3.25% If Year 3 rates = S\$10,000/mth, Year 4 rates would be (10,000 x 1.0325 = S\$10,325/mth), Year 5 rates would be (10,325 x 1.0325 = S\$10,660/mth)</p> <p data-bbox="416 1294 2051 1410">If Year 1 = 1.5% and Year 2 is -2%, the average Total Wage Change (%) = -0.25% If Year 3 rates = S\$10,000/mth As the % is negative, Year 4 and Year 5 rates would remain as S\$10,000/mth</p> | Contract Period | Firm Period | | | Optional Period* | | | Year 1 | Year 2 | Year 3 | Year 4 | Year 5 | Monthly rate | Tenderer to propose | Tenderer to propose | Tenderer to propose | Upon review | Upon review | Annual cost | Tenderer to propose | Tenderer to propose | Tenderer to propose | Upon review | Upon review |
| Contract Period | Firm Period | | | Optional Period* | | | | | | | | | | | | | | | | | | | | | |
| | Year 1 | Year 2 | Year 3 | Year 4 | Year 5 | | | | | | | | | | | | | | | | | | | | |
| Monthly rate | Tenderer to propose | Tenderer to propose | Tenderer to propose | Upon review | Upon review | | | | | | | | | | | | | | | | | | | | |
| Annual cost | Tenderer to propose | Tenderer to propose | Tenderer to propose | Upon review | Upon review | | | | | | | | | | | | | | | | | | | | |

| Items to include | Examples of Tender Instructions | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---------------------------------|---|----------------------|------------|----------------------|-------------|-------------|--|--|-----|----------|--------|--------|--------|--------|--------|---|-------------|------------|------------|------------|-------------|-------------|---|------------|------------|------------|------------|-------------|-------------|---|--|------------|------------|------------|------------|------------|---|---|------------|------------|------------|------------|------------|---|--|------------|------------|------------|------------|------------|
| e) Price Schedule (continue) | <p>Note: If buyer expects a surge in demand for security services during the contract period, the tenderer should submit a schedule of rates for such services that may be required during the contract period. Buyers are encouraged to include requirements for new provider to offer no worse-off remuneration packages and to recognise the lengths of service of incumbent workers who they intend to employ under new contract. It is recommended in an OBC security tender to place a relatively heavier weighting on a service provider’s ability to achieve security outcomes followed by the quality of proposed technology solutions. Training and supervision of SOs and track records should be attributed a relatively lower weighting compared to the proposed concept of operations and technology proposals.</p> <p><u>Schedule of Rates for Ad-hoc Security Services</u></p> <p>Tenderer is to submit prices in the Schedule of Rates for adhoc services, manpower and lease of security equipment that might be requested during the contractual period. Any review of contractual demands which require reviews of manpower or services to take reference to rates* established here.</p> <table border="1" data-bbox="421 911 2027 1326"> <thead> <tr> <th colspan="2"></th> <th colspan="5">Per deployment (S\$)</th> </tr> <tr> <th>S/N</th> <th>Services</th> <th>Year 1</th> <th>Year 2</th> <th>Year 3</th> <th>Year 4</th> <th>Year 5</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>SSO (12hrs)</td> <td>To propose</td> <td>To propose</td> <td>To propose</td> <td>Upon review</td> <td>Upon review</td> </tr> <tr> <td>2</td> <td>SO (12hrs)</td> <td>To propose</td> <td>To propose</td> <td>To propose</td> <td>Upon review</td> <td>Upon review</td> </tr> <tr> <td>3</td> <td>Supply of Queue-poles (per set of 10 for 24hrs)</td> <td>To propose</td> <td>To propose</td> <td>To propose</td> <td>To propose</td> <td>To propose</td> </tr> <tr> <td>4</td> <td>Supply of vehicle barricades (per set of 5 for 24 hrs)</td> <td>To propose</td> <td>To propose</td> <td>To propose</td> <td>To propose</td> <td>To propose</td> </tr> <tr> <td>5</td> <td>Supply of X-ray machine (per set for 24hrs)</td> <td>To propose</td> <td>To propose</td> <td>To propose</td> <td>To propose</td> <td>To propose</td> </tr> </tbody> </table> <p>*Rates based on ability to supply surge demand within notice period of three working days.</p> | | | Per deployment (S\$) | | | | | S/N | Services | Year 1 | Year 2 | Year 3 | Year 4 | Year 5 | 1 | SSO (12hrs) | To propose | To propose | To propose | Upon review | Upon review | 2 | SO (12hrs) | To propose | To propose | To propose | Upon review | Upon review | 3 | Supply of Queue-poles (per set of 10 for 24hrs) | To propose | 4 | Supply of vehicle barricades (per set of 5 for 24 hrs) | To propose | 5 | Supply of X-ray machine (per set for 24hrs) | To propose |
| | | Per deployment (S\$) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| S/N | Services | Year 1 | Year 2 | Year 3 | Year 4 | Year 5 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | SSO (12hrs) | To propose | To propose | To propose | Upon review | Upon review | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | SO (12hrs) | To propose | To propose | To propose | Upon review | Upon review | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | Supply of Queue-poles (per set of 10 for 24hrs) | To propose | To propose | To propose | To propose | To propose | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4 | Supply of vehicle barricades (per set of 5 for 24 hrs) | To propose | To propose | To propose | To propose | To propose | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 5 | Supply of X-ray machine (per set for 24hrs) | To propose | To propose | To propose | To propose | To propose | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| Items to include | Examples of Tender Instructions |
|-----------------------------------|---|
| f) Licensing and Competencies | <p>Tenderer must possess a valid licence, obtained through the SACE exercise conducted by the Police Licensing and Regulatory Department (PLRD). SAs which <u>fail</u> the SACE assessment will not have their licences renewed and would be given two (2) months grace period to cease and/or handover operations.</p> <p>Tenderer must submit the required documentary proof of a valid licence throughout the duration of the contract.</p> <p>Tenderer must also keep buyer informed when they are scheduled by PLRD to undertake the SACE assessment.</p> |
| g) Company profile and experience | <p><u>Financial Statements, Registration of Business</u></p> <p>Tenderer must <u>submit</u> the following documents in the tender submission:</p> <ul style="list-style-type: none"> a) Copy of its audited financial statements for the past three years b) Original copy of the information on the latest business profile by the registry of Companies and Business (Singapore) <p><u>Track Record and Expertise</u></p> <ul style="list-style-type: none"> c) Testimonials and project references of relevant past experiences and expertise attained in relation to security outcomes listed in the tender (if available). This can include reviews from past customers and additional information on the scale of operations and the relevancy of each experience. Reference checks may be conducted. d) Training and competency assessment plans that are established to manage competency of all SOs. This should be supported by evidence of training course attendance or related documents. HR plans and company policies to sustain working conditions that promote work-life balance and measures to ensure officers do not exceed mandated working hours. |

| Items to include | Examples of Tender Instructions |
|------------------------|--|
| h) Evaluation Criteria | <p><u>Cardinal Criteria</u></p> <p>Tenderer must comply with all the requirements and document submissions listed in the Tender Instructions. Any Tender Offer that does not comply with any of the requirements listed below shall be disqualified from further evaluation.</p> <p>a) Attendance at tender briefing and site visit; b) Complete submission of documents listed in the Tender Instructions; and c) Complete submission of Price Schedule.</p> <p><u>Evaluation Criteria</u></p> <p>All Tender Offers shall be evaluated using the Price-Quality Method (PQM).</p> <p>Price evaluation will be performed using the lowest price submitted as comparison across all Tender offers.</p> <p>Quality evaluation will be performed using the following criteria (listed in order of decreasing importance):</p> <p>a) Quality of proposed security solutions – ability to achieve higher levels of security outcomes. b) Quality of technology solutions – maturity of technology solutions and measures made to prepare for deployment of technology solutions. c) Track records – relevance of past experience, expertise in dealing with security operations. d) HR and training competency policies – Tenderer’s commitment to create sustainable and conducive working environment for its officers.</p> |

| Items to include | Examples of Tender Instructions | | | | | | | | | |
|-------------------|--|-------------|---------------|-------------|--|--|--|--|--|--|
| i) Clarifications | <p>There will be a tender briefing and site visit two weeks after the release of the Tender. All interested parties must attend the tender briefing and site visit.</p> <p>After tender closure, the buyer may require the tenderers to conduct a brief on their proposal to the TEC. Details of these sessions shall be finalised after tender closure.</p> <p>For clarifications of tender requirements and registration for the tender briefing and site visits, please contact the following personnel.</p> <table border="1" data-bbox="416 671 1276 826"> <thead> <tr> <th data-bbox="416 671 703 722">Name</th> <th data-bbox="703 671 990 722">Email address</th> <th data-bbox="990 671 1276 722">Contact No.</th> </tr> </thead> <tbody> <tr> <td data-bbox="416 722 703 774"></td> <td data-bbox="703 722 990 774"></td> <td data-bbox="990 722 1276 774"></td> </tr> <tr> <td data-bbox="416 774 703 826"></td> <td data-bbox="703 774 990 826"></td> <td data-bbox="990 774 1276 826"></td> </tr> </tbody> </table> | Name | Email address | Contact No. | | | | | | |
| Name | Email address | Contact No. | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |



4.2 Sample Scope of Work for Security OBC

This section outlines a list of sample Scope of Work that can be adapted into buyer's tender document.

As the scope of work for every site is unique, the buyer should customise the examples based on an assessment of its security requirements.

| Items to include | Examples of Tender Instructions |
|----------------------|--|
| 1) Definitions | <p>This section contains the scope of work for provision of security services, thereafter, known as “Services”, required by <buyer’s name> thereafter known as “Service Buyer”.</p> <p>The successful tenderer is known as the “Contractor”.</p> <p>Premises which security services are to be rendered will thereafter be known as “Contracted Premises”.</p> |
| 2) Contract Duration | <p>The contract for the provision of services shall be scheduled for a firm period of three years with option period of two years. Schedule of rates established to be valid during the firm period and any extended period.</p> |
| 3) Area of Coverage | <p>The Contracted Premises consist of one block of five-storey office building and a basement carpark (50 lots). The total floor area of the Contracted Premise is approximately 10,000m². There are four lifts serving the six levels (including basement carpark).</p> <p>There are three entrances / exits into the building premises (main building entrance at Level 1 lobby, side gate that leads into the fenced perimeter of the premises and vehicle entrance to the carpark).</p> <p>The main lobby at Level 1 is where visitors register and exchange for visitor passes. The vehicle drop-off point is located outside the main lobby at Level 1. Entrance via the side gate is limited to staff access using staff pass as verification. Vehicle access to carpark is limited to authorised staff and registered visitor vehicles.</p> |

| Items to include | Examples of Tender Instructions |
|----------------------|---|
| 4) Security Outcomes | <p>The security outcomes to be delivered by the Contractor are as follows:</p> <p>a) Access control (persons)</p> <ul style="list-style-type: none"> • Only staff and registered visitors/contractors are to be given access to office levels (Level 2 and beyond). • Only staff with access pass allowed to access the perimeter through side gate during its operating hours. <p>b) Access control (vehicles)</p> <ul style="list-style-type: none"> • Only authorised and registered vehicles are to be allowed access into the basement carpark. <p>c) Visitor management</p> <ul style="list-style-type: none"> • Key visitor details, entry/exit records are to be recorded and made available for Service Buyer’s review at any time • All visitors shall be given visitor identification (device/pass/label) and made to don the identification means which identifies them to the building. <p>d) Infrastructural protection</p> <ul style="list-style-type: none"> • Project and maintain security presence as a form of deterrence • Ensure security and safety of persons in the Contract Premises • To detect, record and report potential security incidents in the Contract Premises <p>List of security incidents include:</p> <ul style="list-style-type: none"> - Intrusion and break-in to premises and office floors - Presence of suspicious persons loitering within the premises - Theft - Fire - Unattended equipment and items within premises - Conduct of illegal activities - Incident reports made by staff |

| Items to include | Examples of Tender Instructions | | | | | | | | |
|---------------------------------|--|-------------------|--|-------------------|---------|---|---|------------------|--|
| 4) Security Outcomes (continue) | <ul style="list-style-type: none"> All security incidents to be recorded and made available for reference at any time, incident reports to be saved as record and emailed to Service Buyer's security in-charge (IC) after reports are lodged. Ability to respond up to two concurrent incidents within 5 minutes during office hours and one incident during within 15 minutes during silent hours. Incidents to be reported to Police if required. <p>e) Contingency response</p> <ul style="list-style-type: none"> During emergencies or drills (e.g. fire incident evacuation), to correctly execute contingency response duties as directed by established SOPs. Assist in conduct of drills or participation in exercises when requested. | | | | | | | | |
| 5) Operational Hours | <p>The operational hours for the different areas of coverage are as follows:</p> <table border="1" data-bbox="416 837 2031 1307"> <thead> <tr> <th>S/N</th> <th>Coverage Areas</th> <th>Operating Periods</th> <th>Remarks</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Building perimeter, stairwells and building floor lobbies</td> <td>24hrs (all days)</td> <td> CCTVs are installed in building premises, images piped back to Security Post at main entrance. <u>Internal:</u> Main visitor entrance, Level 1 lift lobby, Building floor lobbies, Stairwell entrance at Level 1 <u>External perimeter:</u> Entrance of access ramp to vehicle entrance, Car park gantry Stairwell entrance door is a single access door that can only be opened from stairwell side. </td> </tr> </tbody> </table> | S/N | Coverage Areas | Operating Periods | Remarks | 1 | Building perimeter, stairwells and building floor lobbies | 24hrs (all days) | CCTVs are installed in building premises, images piped back to Security Post at main entrance. <u>Internal:</u> Main visitor entrance, Level 1 lift lobby, Building floor lobbies, Stairwell entrance at Level 1 <u>External perimeter:</u> Entrance of access ramp to vehicle entrance, Car park gantry Stairwell entrance door is a single access door that can only be opened from stairwell side. |
| S/N | Coverage Areas | Operating Periods | Remarks | | | | | | |
| 1 | Building perimeter, stairwells and building floor lobbies | 24hrs (all days) | CCTVs are installed in building premises, images piped back to Security Post at main entrance. <u>Internal:</u> Main visitor entrance, Level 1 lift lobby, Building floor lobbies, Stairwell entrance at Level 1 <u>External perimeter:</u> Entrance of access ramp to vehicle entrance, Car park gantry Stairwell entrance door is a single access door that can only be opened from stairwell side. | | | | | | |

Items to include

Examples of Tender Instructions

5) Operational Hours (continue)



| S/N | Coverage Areas | Operating Periods | Remarks |
|-----|--|---|---|
| 2 | Main building entrance | 24hrs (all days) | <p>Separate processing channels for staff and visitor entries.</p> <p><u>Peak period for entry:</u> Weekdays excluding public holidays (0800-0930hrs, 1630-1800hrs)</p> <p><u>Peak visitor volume:</u> 100 persons per hour</p> <p><u>Normal office hours visitor volume:</u> not exceeding 20 persons per hour</p> |
| 3 | Side gate | Weekdays (0700-1900hrs) excluding public holidays | Only accessible by staff using staff pass as verification. A single access turnstile is installed at the entrance. |
| 4 | Vehicle entrance and access to carpark | 24hrs (all days) | Only accessible by authorised staff and registered visitor vehicles. Not more than 50 visitor vehicles/day during office hours. An electronic gantry system with intercoms is installed, gantry can be controlled from Security Post at main entrance. |
| 5 | Vehicle drop-off point | Weekdays (0700-1900hrs) less public holidays | This is a public access area that is to be blocked outside of operating periods. |
| 6 | Building Fire Command Centre | 24hrs (all days) | Located inside Security Post at main entrance. |

Note: Office hours is defined as weekdays excluding public holidays (0700-1900hrs).
 Silent hours operation is defined as 1900hrs – 0700hrs (next day), weekends and public holidays.

| Items to include | Examples of Tender Instructions |
|--------------------------|--|
| <p>6) Other Services</p> | <p>In addition to security services, Contractor shall perform the following:</p> <p>a) Manage the administration of the premise staff access system</p> <ul style="list-style-type: none"> • Registration of new staff • Issuance of staff pass to new staff • Destruction of staff pass returned by Service Buyer’s HR office <p>b) Operate the vehicle carpark gantry system</p> <ul style="list-style-type: none"> • Handle and correctly respond to intercom requests • Manually override the system if system is faulty <p>c) Monitor and report security system (non-Contractor Furnished Equipment) or infrastructural failure to Service Buyer’s security IC</p> <p>d) Operate the Fire Command Centre on premises</p> <p>e) Traffic control at drop-off point</p> <ul style="list-style-type: none"> • To ensure smooth and unobstructed use of vehicle drop-off point during office hours <p>Any non-listed services requested beyond the scope of the current contract with corresponding cost adjustments (if required) as a result of additional resources required will be mutually agreed before commencement of services.</p> <p>Note: The above services may not apply to all types of security contracts. Buyers can adopt the examples according to their requirements.</p> |



| Items to include | Examples of Tender Instructions |
|---|---|
| <p>7) Supply and Management of Contractor Furnished Equipment (CFE)</p> <p><i>CFE includes any hardware which is proposed by Contractor for the fulfilment of the contractual requirements. (For example: Handheld metal detectors, CCTVs etc).</i></p> | <p>Contractor shall bear all costs in relation to installation, operational use, maintenance, management and removal of CFE supplied under this contract. Service Buyer shall not be responsible for any loss or damages to any Contractor's equipment held in the Service Buyer's premises.</p> <p>Note:</p> <p>Buyers may also want to include clauses that allow them to buy over CFEs provided by the Contractor at end of the contract period at depreciated costs. Buyers who wish to undertake this should be mindful of technology obsolescence, cost of maintaining aging equipment and availability of service providers to upkeep the equipment thereafter.</p> |
| <p>8) Additional Obligations</p> <p><i>Note: The above obligations may not apply to all types of security contracts. Service buyers can adapt the examples according to their requirements.</i></p> | <p>Contractor is to fulfil the following obligations as part of the security services provided under the contract:</p> <p>a) Training and competency demands</p> <p>Contractor shall ensure all SOs deployed have relevant security qualifications for them to operate effectively in their deployment locations. Contractor is to ensure competency via conduct of refresher or recurrent training which will be done at Contractor's cost. Contractor shall have a system which tracks the qualification and training status of officers deployed. Such information must be made available for audit by the Service Buyer upon request.</p> |

| Items to include | Examples of Tender Instructions |
|---|--|
| <p>8) Additional Obligations (continue)</p> | <p>b) Code of conduct</p> <p>SOs deployed are to abide by the following Code of Conduct. Service Buyer reserves the rights to relieve officers from duty if there is any infringement of requirements, which may otherwise result in serious consequence(s) for the Service Buyer.⁶ It is also the Contractor’s responsibility to seek replacements at no additional cost to the Service Buyer, failing which the Service Buyer will have the right to recover the cost for the relieve officers including any cost in relation to the infringement.</p> <ul style="list-style-type: none"> • While on duty, to be in official attire with identifications passes or badges. Passes or badges to bear Contractor’s company name, officer’s photograph and name of the officer. • To remain alert and vigilant, officers are not to be found sleeping while on duty. • Remain professional in dealing with persons they come in contact with during their duties. • Alert the Service Buyer of any law and order, security incidents without delay. <p>c) Safety and liability</p> <p>Contractor shall at all times observe and comply with all applicable laws and regulations, in particular those relating to safety, and shall bear all costs and expenses connected with the compliance of such laws and regulations. Contractor shall take all reasonable safety precautions to mitigate risk when delivering services. Such precautions include providing and ensuring the use of protective personal equipment where appropriate. Contractor shall effect and maintain adequate policies of insurance in respect of Work Injury Compensation/Employer’s Liability and Public Liability.</p> <p>d) Conduct of audit</p> <p>Contractor shall commit to the regular conduct of audits and inspections at Contracted Premises. A monthly audit schedule will be established together with Service Buyer and Contractor shall ensure that activities are carried out in accordance to schedule and in the presence of Service Buyer’s representative at no additional cost to Service Buyer.</p> |

⁶ Service Buyers should consider the Tripartite Guidelines on Fair Employment Practices (TGFEPP) guidelines, ensure that due process is being accorded, and allow sufficient opportunities for clarification between the service buyer and contractor before making a request to relieve the SO.

| Items to include | Examples of Tender Instructions |
|---|--|
| <p>8) Additional Obligations (continue)</p> | <p>e) Personal data protection</p> <p>Contractor to ensure compliance with the Data Protection Provisions of the Personal Data Protection Act (PDPA) in relation to the personal data collected, used or disclosed as part of contracted services. For example:</p> <ul style="list-style-type: none"> • Ensure individuals are notified and consent is obtained for the purposes of the collection, use or disclosure of their personal data, including NRIC number (unless the collection, use or disclosure is required under any law or an exception under the PDPA applies). • Ensure reasonable security arrangements to protect the personal data in its possession or under its control to prevent any unauthorised access, collection, use, disclosure or similar risks. Given the risks and potential impact of any unauthorised use or disclosure of personal data associated with the individual’s NRIC number, ensure a higher level of security to protect the NRIC numbers (or copies of NRIC) in its possession or under its control. Contractor may wish to consider collecting partial NRIC numbers (i.e. up to last 3 digits and checksum) in place of the full NRIC number, and to consider employing technological solutions, such as scanning of physical NRICs to capture the NRIC number and store the data in a secure manner. • Facilitate any requests for access to individual’s personal data and information about the ways his personal data has been used or disclosed in the past year, unless they fall under one of the prohibitions to access or an exception under the PDPA applies. • Cease retention of the personal data, or remove means by which personal data can be associated with particular individuals, when no longer necessary for any business or legal purpose. <p>Contractors can also refer to the below PDPC resources (found in www.pdpc.gov.sg) for more information when developing and implementing operations involving the collection of personal data:</p> <ul style="list-style-type: none"> • Guide on the responsible use of biometric data in security applications • Guide to securing personal data in electronic medium • Guide to managing data breaches • Guide to disposal of personal data on physical medium • Advisory guidelines on photography, video and audio recordings |

| Items to include | Examples of Tender Instructions | | | | | | | | | | | | |
|--|--|-------------------|-----------|--|---|--|---|-----------------------------------|--|--|--|---|---|
| 8) Additional Obligations (continue) | <p>f) Tripartite Guidelines on Fair Employment Practices (TGFEF) Contractor to ensure compliance to the Tripartite Guidelines on Fair Employment Practice. The guidelines can be found at the Tripartite Alliance for Fair & Progressive Employment Practices (TAFEP) website. https://www.tal.sg/tafep/getting-started/fair/tripartite-guidelines</p> | | | | | | | | | | | | |
| 9) Performance Management and Payment | <p><u>Performance evaluation matrix</u> Contractual performance shall be measured through the performance matrix at Section 4.3 which dictate the acceptable service levels for different security outcomes, as well as corresponding monthly payment schedule. Contractor shall tabulate the monthly performance for Service Buyer’s verification to process monthly payments.</p> <p><u>Service Failures</u> Service Failures are defined as:</p> <table border="1" data-bbox="421 836 2036 1441"> <thead> <tr> <th data-bbox="421 836 1220 879">Security Failures</th> <th data-bbox="1220 836 2036 879">Indicator</th> </tr> </thead> <tbody> <tr> <td data-bbox="421 879 1220 978">a) Unregistered visitors given access to office levels</td> <td data-bbox="1220 879 2036 978">> 15 incidences of visitors found not registered in visitor records</td> </tr> <tr> <td data-bbox="421 978 1220 1077">b) Failure to detect, record, report and prevent incidents resulting in injury to persons, loss / damage of property</td> <td data-bbox="1220 978 2036 1077">Any security incident resulting in injury to persons, loss / damage of property as a result of service lapses</td> </tr> <tr> <td data-bbox="421 1077 1220 1176">c) Failure to keep proper records</td> <td data-bbox="1220 1077 2036 1176">> 25 detected incomplete or missing records (e.g. incident reports, visitor records)</td> </tr> <tr> <td data-bbox="421 1176 1220 1307">d) Failure to perform according to SOP leading to security or safety lapse</td> <td data-bbox="1220 1176 2036 1307">> 8 incidences of incident response that exceeds: • 5 minutes (office hours) • 15 minutes (silent hours)</td> </tr> <tr> <td data-bbox="421 1307 1220 1441">e) Failure to maintain adequate and security presence</td> <td data-bbox="1220 1307 2036 1441">< 60% of days with no deployment shortfall Measured as follows: (number of days with no deployment shortfalls/total number of operational days) x 100%</td> </tr> </tbody> </table> | Security Failures | Indicator | a) Unregistered visitors given access to office levels | > 15 incidences of visitors found not registered in visitor records | b) Failure to detect, record, report and prevent incidents resulting in injury to persons, loss / damage of property | Any security incident resulting in injury to persons, loss / damage of property as a result of service lapses | c) Failure to keep proper records | > 25 detected incomplete or missing records (e.g. incident reports, visitor records) | d) Failure to perform according to SOP leading to security or safety lapse | > 8 incidences of incident response that exceeds: • 5 minutes (office hours) • 15 minutes (silent hours) | e) Failure to maintain adequate and security presence | < 60% of days with no deployment shortfall Measured as follows: (number of days with no deployment shortfalls/total number of operational days) x 100% |
| Security Failures | Indicator | | | | | | | | | | | | |
| a) Unregistered visitors given access to office levels | > 15 incidences of visitors found not registered in visitor records | | | | | | | | | | | | |
| b) Failure to detect, record, report and prevent incidents resulting in injury to persons, loss / damage of property | Any security incident resulting in injury to persons, loss / damage of property as a result of service lapses | | | | | | | | | | | | |
| c) Failure to keep proper records | > 25 detected incomplete or missing records (e.g. incident reports, visitor records) | | | | | | | | | | | | |
| d) Failure to perform according to SOP leading to security or safety lapse | > 8 incidences of incident response that exceeds: • 5 minutes (office hours) • 15 minutes (silent hours) | | | | | | | | | | | | |
| e) Failure to maintain adequate and security presence | < 60% of days with no deployment shortfall Measured as follows: (number of days with no deployment shortfalls/total number of operational days) x 100% | | | | | | | | | | | | |

| Items to include | Examples of Tender Instructions |
|---|---|
| <p>9) Performance Management and Payment (continue)</p> | <p><u>Incentive sharing</u> Contractor shall commit to an incentive sharing arrangement where incentives are equally shared between the Contractor and its officers operating on the Contracted Premise. Service Buyer shall have the rights to interview Contractor’s officers or review finance information to verify compliance.</p> <p>Note: There is no specific rule-of-thumb amount for incentive sharing. Buyers can choose to include the clause based on their requirements.</p> <p><u>Performance review meetings</u> For the purpose of reviewing contract performance and operational demands, review meetings shall be conducted when requested by the Service Buyer. The review meetings shall be held at the Contracted Premises. Each party shall bear its own costs and expenses in respect of the review meetings.</p> <p><u>Termination due to poor performance</u> Service Buyer has the rights to issue warning letters or to terminate contract if there is persistent poor performance resulting in three consecutive months of Service Failure conditions being recorded. If termination is exercised under this condition, Contractor shall be issued with a minimal three-month notice.</p> <p><u>Productivity Enhancement Framework</u> Contractor shall continue to review possibilities of enhancing productivity or security outcomes during the contract period and submit proposals which can lead to tangible enhancements to Service Buyer for consideration. If Service Buyer decides to implement any proposal, it shall initiate discussions with Contractor on the implementation and finance details. Nett cost savings achieved as part of proposal implementation shall be shared between Service Buyer and Contractor.</p> <p>Note: There is no specific rule-of-thumb amount to achieve as it varies depending on the nature of the proposal. The amount of cost savings shared should be determined after discussions with Tenderer.</p> |



| Items to include | Examples of Tender Instructions |
|--|--|
| <p>10) Obligation for Contract Reviews</p> | <p><u>Periodic reviews</u></p> <p>Service Buyer reserves the rights to perform periodic reviews of contracted scope (at least once per contract year). Such reviews will be performed together with the Contractor. Changes to be executed through contract variations and reasonable lead time shall be given to Contractor for any transition.</p> <p>In the event where unforeseen circumstances (e.g. changes or introduction of new government policies) affecting resourcing and cost of services are introduced, it shall be Contractor’s responsibility to put up proposals for pricing or operational deployment changes for Service Buyer’s review. Proposals for changes in pricing must be substantiated with facts which are to be accepted by Service Buyer before any contractual changes takes place. If Service Buyer and Contractor are unable to reach consensus on the price review amount, the matter should be brought to arbitration or mediation. In the event where no consensus can be reached, Contractor has the option to exercise Termination in accordance with the mutually agreed termination period.</p> <p><u>Surges and Contingencies</u></p> <p>Contractor shall be obligated to support surge and contingency operations demands defined by the Service Buyer. Such demands which may not be part of original contractual terms is to be developed during the contract period. Additional resources required and its related charges if accepted by the Service Buyer shall be incorporated as part of this Contract via contract variation.</p> |

In addition to clauses seen above, buyers can consider incorporating fair contracting terms in the following areas:

(i) Fees for late payment

In event of late payments not due to default by Contractor, Service Buyer to allow Contractor to claim pro-rated late payment fees based on established business loan rates (e.g. 10.8% per annum).

(ii) Termination

To allow both parties to terminate contract in accordance with mutually agreed notice periods. Parties may take into consideration that either party may require longer notice periods due to internal processes. If deemed necessary to mitigate risk, Service Buyers may also consider defining conditions where rights of termination can be exercised for both parties.

(iii) Price review and co-sharing of saving

Variations for this could consider:

- Fixed % price escalation which can be proposed by Contractor or defined by Service Buyer
- Cost adjustment factors using formulas that take into account different economic indices
- Obligations to review pricing in event of government policy changes which has cost impact on resources (e.g. PWM reviews), or other economic forces such as inflation and manpower shortage
- Obligations to co-share savings in the event Contractor is able to receive technology/productivity grants or subsidies from government for contracted operations

(iv) Dispute resolution

Service Buyer may wish to consider including mediation before forms of dispute resolutions. Buyers may consider specifying the Small Claims Tribunals as a means of settling disputes for claims below \$20,000.

(v) Limitation of Liquidated Damages

A percentage of the monthly contract price should be stipulated as the minimum amount to be paid to the Contractor, after consideration of outcomes. The buyer should also be required to provide evidence of alleged breaches. Security contracts should include a limitation of liquidated damages clause.

An example of such a clause is as follows:

“The Client shall provide the Agency with the details and where applicable, evidence of the underlying breaches for which the Client intends to impose any liquidated damages. The total sum of liquidated damages applied per month shall not, in any event, exceed X% of the monthly contract sum. The said limitation on liquidated damages shall not apply to any shortfall, for which there shall be a deduction from the amount due pro-rated from the contract sum”.

Buyers may also refer to recommendations found in tripartite advisories such as those issued by MOM and SNEF.



4.3 Monthly Performance Evaluation Matrix

Note:

The performance matrix and demerit points models below are purely for reference, buyers can adopt other forms of performance related payment models and adjust the payment sums depending on the nature and criticality of their sites.

| S/N | Performance Outcome | Performance Indicator | Score | | | | | |
|--|--|--|--------------------------|-------------|-------------|-------------|-----------------|---------------------|
| | | | 0 (Security Failure)* | 1 | 2 | 3 | 4 (Baseline) | 5 (Bonus point)† |
| Protection of occupants and property | | | | | | | | |
| 1 | No incidents of unauthorised access in each month | Number of visitors found not registered in Visitor records Note: This can be derived from verified inputs raised by staff or audit checks performed by Service Buyer's security IC. | ≥ 15 | 10-15 | 5-10 | 2-5 | 0 | NA |
| Security with minimal service failure and timely service recovery | | | | | | | | |
| 2 | Overall customer satisfaction of security services of at least 80% | Average % score from feedback surveys collected Note: Provider is to conduct minimum of ten feedback surveys per month. Surveys are to be completed by staff, buyer's security IC or verified visitors / tenants. Survey inputs can cover scope of work defined under "Other services" and scope defined under "Code of conduct". | <50% | 50%- 59% | 60%- 69% | 70%- 79% | 80%- 90% | >90% |

| S/N | Performance Outcome | Performance Indicator | Score | | | | | |
|---|--|--|--------------------------|---------------|---------------|---------------|-----------------|---------------------|
| | | | 0 (Security Failure)* | 1 | 2 | 3 | 4 (Baseline) | 5 (Bonus point)† |
| 3 | System availability of critical Contractor furnished security system to be at least 97%. Note: System maintenance and System failures are considered as system downtime | (System operating time (hrs) / Total Duration of deployment (hrs)) x 100% Note: This assumes Contractor will be providing hardware or systems which are critical to security operations. Data will be tracked from system logs. | <90% | 91%- 92.9% | 93%- 94.9% | 95%- 96.9% | >97% | NA |
| 4 | Ensure number of improper/incomplete records identified <5 | Total number of incomplete or missing visitor records, incident reports found during monthly audit checks | >25 | 15-25 | 10-14 | 6-9 | <5 | NA |
| Sense of security and visible presence | | | | | | | | |
| 5 | 90% attendance of SOs | (Number of days with no deployment shortfalls/Total number of operational days) x 100% Note: Failure to deploy officers for manned post or failure to find replacement of officers for manned post within 2hrs of shift to be deemed as deployment shortfall. | < 60% | 60%- 70% | 71%- 80% | 81%- 89% | 90%- 99% | 100% |
| 6 | Ensure number of incidents where Officers fail to respond within response time | Total number of incident response that exceeds <ul style="list-style-type: none"> 5 minutes (office hours) 5 minutes (silent hours) Note: Number of incidents includes actual incident and drill activations‡ raised by Service Buyer | >8 | 8 | 7 | 6 | 1-5 | 0 |

Note:

* Service Failure conditions resulting 90% payment will apply when any of three conditions occurs:

- a) Monthly score below 12;
- b) Any individual KPI achieving a 0 score; or
- c) Any incident that results in injury to persons, loss/damage of property due to service lapses or failure to follow SOP

† Bonus point to be awarded when the target set is achieved

‡ Minimal of 5 drill activations to be activated per month

Monthly Payment based on Performance Matrix

| Score | Payment |
|-----------------------|---------|
| >26 (Bonus) | 105% |
| 24 – 25 (Baseline) | 100% |
| 18 - 23 | 97% |
| 12 – 17 | 95% |
| <12 (Service Failure) | 90% |



4.4 Demerit Points Model

The Demerit Points Model of assessment measures the performance of contractors based on their failures to meet service standards or performance indicators leading to service/security failures. Service failures are defined as failures that do not lead to serious security incidents. The occurrences of service and security failures will result in the accumulation of demerit points depending on the severity of the failures. An example of demerit points attributed to various service/security failures is presented below:

| Demerit Points | Type of Service/ Security Failure |
|----------------|---|
| 3 | <ul style="list-style-type: none"> • Deployment of unauthorised personnel for operations • Failure to comply with the Code of Conduct • Failure to be properly equipped/attired in relation to contracted requirements • Loss or misuse of official documents or operational data • Failure to provide accurate information to visitors • Failure to report faulty equipment in premise • Negligence leading to loss of keys to access doors • Failure to activate cleaners to clean wet areas during rainy days • Failure to ensure cleanliness of facilities |
| 5 | <ul style="list-style-type: none"> • Deserting post or becoming uncontactable during duty period • Desertion of manned post without authorisation • SO found to be sleeping on duty • Failure to comply with security guidelines/SOP/Directives • Failure to ensure proper locking and unlocking of doors, roller shutters • Failure to detect and report on failures and building defects during daily checks • Failure to switch off power and facilities |

| Demerit Points | Type of Service/ Security Failure |
|----------------|--|
| 10 | <ul style="list-style-type: none"> • Failure to detect, report and activate response to crime or security incident • Failure to ensure no congestion occurs in drop-off point due to waiting vehicles, • Failure to ensure no vehicle stops at the drop off point for more than 2 minutes • Failure to prevent illegal parking and waiting at the drop off point. • Customer satisfaction level from customer feedback is less than 80% |
| 20 | <ul style="list-style-type: none"> • Failure to respond to on-site incidents within X minutes of activation • Improper change of security pass • Monthly attendance is between 92-97% • Availability of critical technology solution is less than 85% (if applicable) |
| 40 | <ul style="list-style-type: none"> • Monthly attendance is lower than 92% • Failure to detect and prevent the occurrence of illegal activities including gambling and unauthorised hawking • Criminal conduct while on duty |
| 50 | <ul style="list-style-type: none"> • Negligence resulting in failure to detect or prevent incidences of injury • Failure to detect critical incidents such as break-ins, burglaries, vandalism, thefts and fire etc. |

Note:

Monthly attendance = 100% - [(Total No. of shift deployments with absentee within a month/ Total no. of shift deployments operated following the Resource plan within a month)] x 100%

(Failure to report within 2hr of deployment time will be deemed as an absent incident. Monthly attendance results will be rounded down to the nearest whole number)

If service and/or security failures occurs due to poor or non-compliant services rendered by the Contractor during the Measurement Period, demerit points will be issued to the Contractor. The issuance of demerit points will impact the monthly payment sum. An example of the accumulation of demerit points leading to the determination of the monthly payment sum is presented in table below.

Demerit Point scale

| Demerit point scale | Impact on Payment sum |
|----------------------------|--|
| <10 points | 5% above full payment (bonus) |
| 10-19 points | Full payment sum |
| 20-29 points | 3% deduction off payment sum |
| 30-49 points | 5% deduction off payment sum |
| ≥ 50 points | 10% ⁷ deduction off payment sum |

⁷ Buyers are encouraged not to exceed 10% deduction as it may impact the SA's operational viability such as payment of salaries to SOs.



4.5 Tender Evaluation

This section shows a sample Tender Evaluation Report. Buyers should perform this in relation to what has been defined in Tender Instructions and agreed by the Tender Evaluation Committee (TEC).

Scope of Evaluation

1. A tender for the provision of security services at <Contracted Premises> was called on <Date>. At the close of the tender on <Date>, five tender proposals were received. A TEC comprising of the following members was formed to evaluate the proposals:

| Name | Designation | Evaluation committee |
|------|-------------|----------------------|
| | | Chairman |
| | | Member |
| | | Member |

Stage 1 Evaluation: Cardinal Requirements

2. The TEC adopted a two-stage evaluation process. In Stage 1, Tenderers are assessed on their compliance with the cardinal requirements in the tender document. Only those who have met the requirements in Stage 1 evaluation will proceed to Stage 2 evaluation.

3. Table 1 below shows the comparison of the five proposals under Stage 1 evaluation. Tenderer D had registered interest for the Tendering Briefing but did not attend the Briefing as shown in the Tender Brief attendance records. Tenderer E has submitted an incomplete price schedule without a resource plan. As such, Tenderers D and E have failed to meet all the Cardinal Requirements specified in the tender and will be disqualified from Stage 2 evaluation.

Table 1

| S/N | Cardinal Criteria | Tenderers | | | | |
|-----|---|-----------|---|---|---|---|
| | | A | B | C | D | E |
| 1 | Attendance in Tender Brief | Y | Y | Y | N | Y |
| 2 | Complete submission of specified Tender documents | Y | Y | Y | Y | N |
| 3 | Complete submission of Price Schedule | Y | Y | Y | Y | N |

Note: "Y" denotes compliance with cardinal criteria. "N" denotes non-compliance with cardinal criteria.

Stage 2 Evaluation: Price-Quality Method (PQM)

4. Only three Tender Offers have met the cardinal requirements in Stage 1 evaluation and will proceed to Stage 2 evaluation using the Price-Quality Method (PQM). A weighted assessment of 40% Price and 60% Quality was adopted for Stage 2 Evaluation.

Price Evaluation

5. Price evaluation was performed using the lowest price submitted by Tenderer C as comparison across all Tender offers. The P-Score* for the three tender proposals is in Table 2 below:

Table 2

| | Tenderer A | Tenderer B | Tenderer C |
|------------------------|-------------------|-------------------|-------------------|
| Price submitted | \$1,100,000 | \$900,000 | \$750,000 |
| Weighting | 40% | 40% | 40% |
| P-Score | 0.27 | 0.33 | 0.40 |

* P-Score = [Lowest Tenderer Proposal cost / Tenderer's offered Proposal cost] x Price Weighting

Quality Evaluation

6. Quality evaluation was performed using the following criteria with the corresponding weighting (listed in order of decreasing importance):

| Quality Criteria | Weighting |
|--|------------------|
| Quality of proposed security solutions | 40% |
| Quality of technology proposals | 30% |
| Track records | 20% |
| HR and training competency policies | 10% |

7. The TEC scored each criterion using the 3-point rating system (0-3) below:

| Quality Criteria | Rating (on a scale of 0 to 3) |
|--|---|
| Quality of proposed security solutions | <p>0 - Proposed solution will achieve security outcomes which are worse-off than current operations.</p> <p>1 - Proposed solution will achieve security outcomes similar to current operations.</p> <p>2 - Proposed solution will achieve better security outcomes in at least 1 area with no deterioration in other remaining areas.</p> <p>3 - Proposed solution will achieve better security outcomes in more than one area with no deterioration in other remaining areas.</p> |
| Quality of technology solutions | <p>0 - No technology solution was proposed</p> <p>1 - Proposed solutions does not help to achieve security outcomes or enhance productivity.</p> <p>2 - Technology solutions are untested but will help to achieve security outcomes or enhance productivity.</p> <p>3 - Technology solutions are matured, in-use or qualified technologies that will help achieve security outcomes or enhance productivity.</p> |
| Track records | <p>0 - Does not meet any of the three track record review areas</p> <p>1 - Meets any one of the three track record review areas</p> <p>2 - Meets any two of the three track record review areas</p> <p>3 - Meets all three track record review areas</p> <p>The three track record review areas are:</p> <ul style="list-style-type: none"> • Track record of performing operations with contract value of at least (\$XXX) • Past track record of performing operations of similar nature • Past customer review of services performed |
| HR and training competency policies | <p>0 - Proposed or have established HR processes in one area</p> <p>1 - Proposed or have established HR processes in two areas</p> <p>2 - Proposed or have established HR processes in three areas</p> <p>3 - Proposed or have established HR processes in four areas</p> <p>The four areas are:</p> <ul style="list-style-type: none"> • Training and development plans to maintain and enhance competency of SOs • Individual career development plan for SOs • Rewards and recognition practices for good performance • Work-life balance initiatives and measures to ensure officers do not exceed mandated working hours limit |

8. The individual Q-Scores of the tenderers are tabulated below to compare the quality of the proposals amongst the three tenderers. Tenderer A achieved the highest Q-point of 2.4/3.

| Quality Criteria | Tenderer A | | Tenderer B | | Tenderer C | |
|--|------------|----------|------------|----------|------------|----------|
| | Score | Q-Points | Score | Q-Points | Score | Q-Points |
| Quality of proposed security solutions (40%) | 3 | 1.2 | 2 | 0.8 | 1 | 0.4 |
| Readiness of technology solutions (30%) | 2 | 0.6 | 2 | 0.6 | 1 | 0.3 |
| Track records (20%) | 2 | 0.4 | 3 | 0.6 | 2 | 0.4 |
| HR and Training competency policies (10%) | 2 | 0.2 | 3 | 0.3 | 2 | 0.2 |
| Total Q-Points* | 9 | 2.4 | 10 | 2.3 | 6 | 1.3 |
| Q-Score† | 0.60 | | 0.57 | | 0.32 | |

* Q-Points = [Score x Weightings]

† Q-Score = [Tenderer Total Q-point / Highest Total Q-point amongst Tenderers] x Quality Weighting

Recommendation for Award

9. The total combined score calculated based on the price and quality assessment of the three proposals is tabulated below. Tenderer B scored the highest and is recommended for award.

| | Tenderer A | Tenderer B | Tenderer C |
|--------------------|------------|-------------|------------|
| P-Score | 0.27 | 0.33 | 0.40 |
| Q-Score | 0.60 | 0.57 | 0.32 |
| Total Score | 0.87 | 0.90 | 0.72 |

Section 5:

List of Resources

The list below is a compilation of security outcome-based contracting and related resources for easy reference.

| S/N | Resource | Link |
|-----|---|--|
| 1 | Security Outcome-based Contracting Portal: <ul style="list-style-type: none">• Grants for technology adoption• OBC related courses• Outcome-based contract templates• OBC resource kit for private residences | https://www.police.gov.sg/Advisories/Security-Outcome-Based-Contracting/Security-Outcome-Based-Contracting |
| 2 | Progressive Wage Model | https://www.ntuc.org.sg/tripartiteguidelines |
| 3 | Guidelines for Enhancing Building Security in Singapore | https://www.police.gov.sg/Advisories/Infrastructure-Protection/Building-Security |
| 4 | List of Industry-Accredited Security Consultants | https://scap.info |
| 5 | Security Industry Digital Plan | https://www.imda.gov.sg/programme-listing/smes-go-digital/industry-digital-plans/security-idp |
| 6 | Security Agencies Competency Evaluation (SACE) | https://www.police.gov.sg/e-Services/Police-Licences/Security-Agencies-Competency-Evaluation |
| 7 | Tripartite Guidelines on Fair Employment Practices (TGFE) <ul style="list-style-type: none">• 1st link: Website• 2nd link: PDF | https://www.tal.sg/tafep/getting-started/fair/tripartite-guidelines https://www.tal.sg/files/tripartite-guidelines.pdf |
| 8 | Personal Data Protection Commission Resources: <ul style="list-style-type: none">• Guide on the responsible use of biometric data in security applications• Guide to securing personal data in electronic medium• Guide to managing data breaches• Guide to disposal of personal data on physical medium• Advisory guidelines on photography, video, and audio recordings | https://www.pdpc.gov.sg |

| S/N | Resource | Link |
|-----|--|--|
| 9 | <p>Security Productivity Initiative (SPI)</p> <p>The SPI includes initiatives such as Support for Job Redesign under Productivity Solutions Grant (PSG-JR), Career Conversion Programme (CCP) for Security Officers (SOs), and Guide to Security Workforce Transformation.</p> | <p>https://www.wsg.gov.sg/programmes-and-initiatives/security-productivity-initiative.html</p> |