



Introduction to Purchasing Security

THE
CHARTERED INSTITUTE OF
PURCHASING & SUPPLY





Introduction to Purchasing Security

The key objective of this briefing is to bridge the gap of the complexities involved in buying security services. This has been achieved by incorporating the experiences and perspectives of both parties.

The UK security sector is currently undergoing a period of rapid legislative change. Against a background when security and procurement professionals were found to have misunderstandings about each others role, a guide to good practice aimed at both groups was viewed as timely.

Executive Summary

Chief executives look to purchasing and supply management to control costs and manage risks by removing vulnerabilities in the value chain. These are no less important when buying security.

One of the important messages is that procurement is not an isolated activity within the organisation and when it comes to security many representatives should be brought together to help inform the buying decision. For example, facilities management are often linked to the provision of security, so taking account of their requirements is crucial.

The key to good security is to develop a robust risk profile that considers the impact of all the security risks upon all aspects of the business, ensuring that the security provision has an appropriate balance between technological and human resources. Clearly, security services need to be cost effective and proportionate to the risk. The following must be taken into account:-

- **Project definition**

Defining the security requirements is one of the vital elements of the procurement process. The proposed specification needs to be treated as a serious communication device that allows the security provider to gain a good understanding of what is required.

- **Prequalification**

Prequalification criteria need to be broad and cover at least the following: Details of the security provider's organisation, the commercial aspects of the offering and

contract management philosophy. All of which will encourage security providers to become superb suppliers and build unconditional trust with the client organisation. The client organisation should be adaptable and should bring no surprises.

- **Contract negotiation**

When negotiating a contract for a security provision, careful consideration will need to be given as to the types of clauses used. For example, many clauses used in service contracts are generally termed boilerplate clauses, however, attention needs to be given to more substantive clauses that will need to be embedded into the contract.

- **Contract management**

- Service Level Agreements (SLAs) are critical to the success in defining the relationship between the client organisation and its security provider. It is becoming an increasingly important document as it defines the basic functional parameters such as service and quality.
- Key Performance Indicators (KPIs) are critical in all security agreements. It ensures that the client organisations expectations are not only defined, but KPIs also serve to explain to the security provider how their performance will be appraised.

In conclusion, it is important that all parties involved in the procurement of security services understand:-

- The nature of security risks and the precise impact that security measures can make.
- The benefit of using accredited suppliers.

- Whether those that quote the minimum price can deliver on all aspects of the contract.
- The veracity of tender documents.
- Setting meaningful communication.
- What you can get from a good supplier that you will not from a bad one.
- Why an overarching security strategy is important.
- How to get behind the sales pitch.

This business briefing on purchasing from the security services sector has been developed to alert both security services and purchasing & supply management (P&SM) professionals of the common aspects of good practice.

1. Introduction

Globalisation has brought about a rapid and extensive change in the way organisations operate. This change will increase opportunities for wealth and well-being but also create new channels for risk and insecurity.

Business leaders are looking at ways to improve their own organisational readiness and responsiveness to address the above which are further complicated by issues such as pandemics, terrorism, natural disasters and even cyber threats.

Ensuring organisations have the right balance between the ability to mitigate threats and the ability to respond to them is crucial for doing business in the 21st century. Organisations who maintain this fine balance will have the ability to weather the increasingly complex business environment.



Introduction to Purchasing Security

There is a growing need to ensure that an organisation's security provision adopts a proactive approach to the protection of tangible and intangible assets not only within your own organisation but also the supply chain you operate in. As organisations continue to outsource services or even establish physical assets in this more complex business environment the protection of both tangible and intangible assets will require a more strategic approach to buying security services.

The UK security market now has an approximate net worth of £3 billion - £4 billion per annum, and this looks set to rise according to Professor Martin Gill of Perpetuity Research & Consultancy Ltd (PRCI). Professor Gill argues that 43 per cent of organisations involved in buying security had seen a visible increase in security spend as opposed to just 8 per cent who had seen a decline. He also states that 25 per cent of organisations involved in the research were planning to further increase their security spend, outnumbering those organisations planning to reduce it.

In response The Chartered Institute of Purchasing & Supply (CIPS) are partnering with Perpetuity Research & Consultancy International (PRCI) who are spearheading the Security Research Initiative (SRI). This initiative is supported by The Security Institute (TSI), The British Security Industry Association (BSIA) and ASIS International. The SRI members include, Case Security, CMP, HSBC, Initial Security, Johnson Controls, KPMG, Norbain, OCS-Resolution, Securiplan, Spinnaker International, The Corps, Wilson James and Wyeth Pharmaceuticals

Together we have produced this business briefing on purchasing from the security services sector to alert both security services and P&SM professionals of the common aspects of good practice when it comes to buying security services. In the wake of recent legislative changes there has never been a better time for such a document.

2. Security & the changing UK landscape

The security services sector in the UK is a growth industry. It covers a range of services from the application of physical hardware to business wide electronic security systems that require administration level operation and management. As well as manned guarding and wheel clamping.

Until recently security services and security systems provision have been seen as tactical and operational and little thought has been given to its strategic intent. For some time key players within the security sector have been working hard to ensure a more professional provision of security services and this is now becoming a reality.

In January 2001 the Private Security Industry Act (PSIA) 2001 was published and the purpose of this legislation was to set up a regulatory body, now known as the Security Industry Authority (SIA). The SIA was set up in April 2003, but the full impact for manned security services did not come about until March 2006. This new legislation dictates that anyone who provides unlicensed contracted security personnel is operating illegally and committing a criminal offence; the penalties for which range from fines to 5 years imprisonment. The effect on the market place of this legislation is difficult to anticipate at this stage. However, it is not inconceivable to expect higher prices and a reduced skilled workforce from which to select manned security providers as a consequence of this uncertainty. Organisations may just disappear off the landscape because of associated costs of licensing or through mergers and acquisitions. This could result in a consolidation of the remaining suppliers, creating a serious vulnerability in supply chains within this sector.

Despite the important role security plays, there has been no regulation to control those who work in the security industry and there has only been voluntary standards to which organisations worked. This has made it

difficult to find the right security provider. In fact, organisations have been owned by people with serious criminal records; it is anticipated as a consequence of PSIA 2001 licensing will bring about an end to this type of malpractice.

In the Information Technology sector, some engineering standards have been developed through the efforts of the BSIA and other industry inspectorates to establish some base line requirements for security systems. These standards are concentrated mainly in the area of Intruder Detection and Remote Monitoring by using graded systems to meet a certain level of security threat such as in the Banking and Financial Sectors versus low level systems for Domestic or Small Retail Systems. These security systems standards have mainly been put in place due to the high number of police call-outs to false alarms or unverified requests to attend a situation reported through unqualified security systems that have not met these stringent standards. Relevant British Standards are BS8418 for alarm verification and BSI PD6662 for installation of intruder systems incorporating BS4737 requiring the use of graded equipment under EN50131 parts 1 to 6.

Understanding the technology and setting up the equipment requires a trained technician or programmer with a logical understanding of the organisation the system is effectively controlling. Trained & qualified staff should be audited to ensure the provider is able to meet the specification or design. The use of consulting engineers is commonplace in security systems but it is difficult to qualify experience in this field of expertise. Membership of an institute or industry association may not be the only recommendation one should seek. For example references from former clients may be a preferred way of qualifying the provider.

Research conducted by PRCI has shown that there is sometimes a gulf between the views of security professionals on the one hand and procurement professionals on the other. The



Introduction to Purchasing Security

security professional's view of procurement professionals is that due to a lack of understanding of either the legislation or practice in the security world they are ignoring good quality security provision in search for the lowest price. On the other hand the procurement professionals view security professionals as unimaginative and all too willing to work for low wages. Clearly this creates an impasse. An objective in producing this guide is to bring the security profession and the procurement profession closer, thus reducing the gulf in opinions, it is hoped that when security providers meet procurement professionals in a commercial situation a meeting of minds will occur as opposed to the most common adversarial type approach.

3. The Approved Contractor Scheme (ACS)

Professionals who work within and alongside the security industry have for sometime been calling for regulation within the security sector. As a result of such calls which included a public consultation period we have now seen the introduction of the Approved Contractor Scheme (ACS). According to the SIA the ACS is seen as a hallmark of quality that will enable buyers of security services to distinguish between potential suppliers quickly, accurately and objectively.

To date the ACS has received positive acclaim from both security and procurement professions; both professions must continue to work together to encourage success and remove from the market any potential rogue traders. In addition some indirect benefits to be derived from such licensing include for example security providers being able to create innovative services built around the needs of clients and technology, and this collaboration will help enhance relationships between both professions.

Below are some comments from professionals in both camps on the introduction of the ACS.

Roy Ayliffe, FCIPS, Director of Professional Practice at CIPS says:

"Procurement professionals will welcome the advancements the security sector has made. Whilst security providers may be ACS accredited and a level playing field is achieved within the market, procurement professionals will need to satisfy themselves that the validity, scope and relevance of the ACS is rigorous. This also applies to assurances of any examination to achieve ACS accreditation is a rigorous one. At the end of the day, it is the procurement professional's organisation at risk if unapproved security providers are found supplying services."

Stuart Lowden, Managing Director, Wilson James says:

"The Approved Contractor Scheme has been advertised as the new benchmark of quality for the security industry. However, there are some who would argue that the NSI Gold qualification and BSIA entry criteria are just as important if one is seeking a reliable security provider. In fairness, it is still too early to assess the relative merits of each set of qualifications. The ACS is still in its infancy so some caution should be exercised before accepting this stamp as a guarantee of quality. However, once the inspection regime is in force (anticipated to start in September 2006) the stamp will become an increasingly meaningful one."

It should be recognised that none of the qualifications, whether ACS, NSI Gold or BSIA membership, are set at the 'best practice' level, this would be commercially and operationally unrealistic. They instead represent practice at a recommended minimum level, one that may be acceptable to some buyers but not to others. Those buyers seeking a higher quality service would be advised to use current standards, including ACS, as a base point only."

This position may change if the SIA decides to raise standards within the ACS in the future. However, given the Government's current move towards reduced regulation, an immediate raising of the bar seems

highly unlikely."

In financial terms, membership of ACS is only marginally more expensive than achieving ISO 9001 and the relevant British Standards, perhaps one or two pence per hour on top of this cost. This is a fraction of the more significant costs of licensing, namely the extra process costs (recruitment, training, licensing processing, licence fee) and of course wage inflation."

4. What does good procurement practice look like?

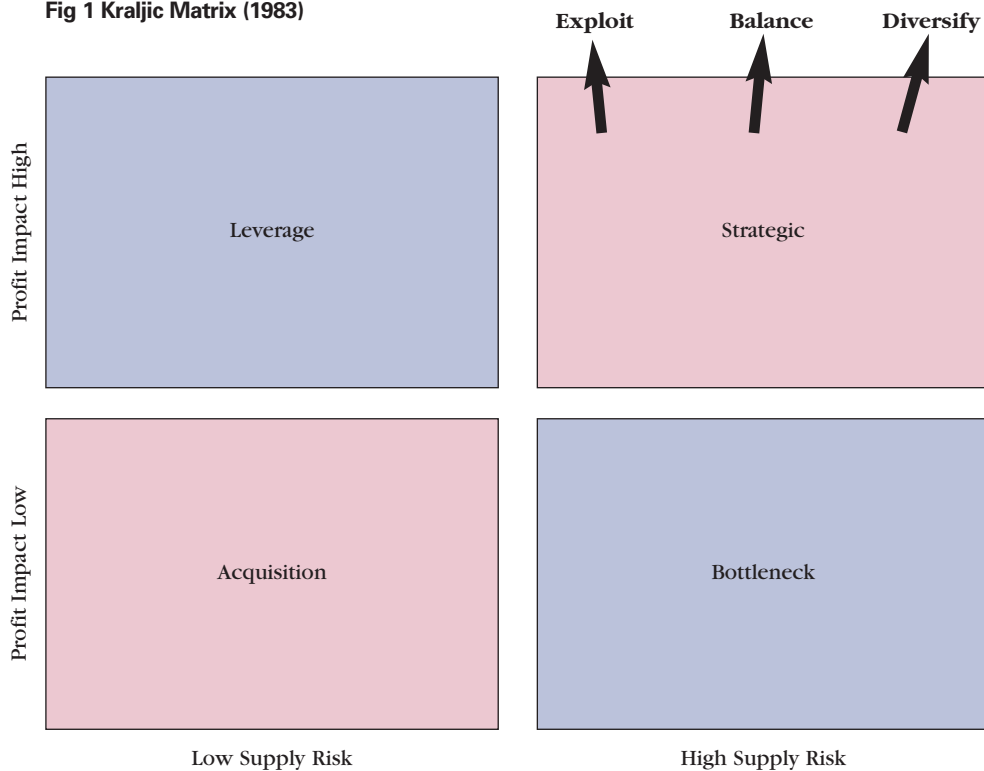
Procurement is not an activity undertaken in isolation. Within business, procurement has become a cross functional activity involving many people. Those people will be engaged and influential at different stages within the procurement process.

However, before any procurement activity commences it is important that all the people involved in the process know and understand the current risk profile for their organisation and adopt a strategic approach to buying security.

By adopting a strategic approach it will move security away from merely reactive responses towards the proactive protection and enhancement of tangible and intangible assets. This will elevate security to become an essential component of a robust risk management system that is fully integrated and aligned with the organisations overall mission and strategy.

Introduction to Purchasing Security

Fig 1 Kraljic Matrix (1983)



4.1. Building a risk profile

All of the people involved in the buying of security need to identify key security risks and assess their own organisations ability to absorb and manage such risks. The first step forward, taken by them or by engaging specialist help, is to build a risk profile of the specific threats and risks faced by the organisation. Some of the key factors that should be considered and perceived as good practice in risk analysis are:

- The level of security risks one can afford to assume in an expanding market
- The level of security needed to control the risks encountered
- The appropriate measures to monitor risks in relation to the level of risk exposure that is considered appropriate and acceptable
- A risk mitigation and recovery strategy that is cost effective.

The building of the security risk profile is just one element of the overall risk profile. Procurement professionals at this stage should now be considering the use of a number of diagnostic tools, such as the Kraljic Matrix

(See Fig 1). This matrix remains the foundation to procurement strategy for many organisations in many sectors.

This particular matrix will enable procurement professionals to understand security services across two dimensions: profit impact and supply risk ('low' and 'high'). The result is a 2x2 matrix and a classification in four categories: bottleneck, non-critical, leverage and strategic items. Depending upon where security services may fit within this portfolio it will require a distinct approach:

- **Acquisition items;** will require efficient processing, product standardisation, order volumes and inventory optimisation.
- **Leverage items;** allow the buying organisation to exploit its full purchasing power, for instance through tendering, target pricing and product substitution.
- **Bottleneck items;** can cause significant problems and risks which can be handled in numerous ways, volume insurance being just one, vendor control and back up plans are others.

- **Strategic items;** further analysis will be required in this area and recommendations would be to plot the buying strengths against the strengths in the security market where three basic power positions will be identified and then associated with three different supplier strategies: balance, exploit and diversify.

The idea behind the Kraljic matrix is to minimise supply risk and maximise buying power. A security provision could feature in any of the four dimensions highlighted above. It is the analysis that emerges from this diagnostic tool that will define what approach is taken when looking at the purchase of a security provision.

4.2. Defining the requirements

Once you have a detailed understanding of your organisations risk profile and before you approach a security provider it is important that you define your particular requirements and the objectives for the security service or system you need to acquire. Defining the requirements is one of the most important elements of the procurement process and should be undertaken carefully and with the support of a cross functional team. If your organisation has many buildings and sites it is highly likely they will all have different security needs.

The specification plays an important role in communicating your requirements to security providers. When this specification is prepared there will be a natural tendency to relate it to current security measures and staffing levels, this is a common error amongst procurement professionals. The result is that the specification becomes too prescriptive and subsequently a lack of innovation is introduced into any future proposal submitted as a result of an Invitation To Tender (ITT).

This particular stage should be seen as an opportunity to start your review with a blank sheet of paper and work out the appropriate level of security for your organisation, irrelevant of the nature of the business. There



Introduction to Purchasing Security

is a need to balance conflicting factors such as potential risks to your business, site accessibility and achieving value for money. For example, if your organisation is in the financial services sector, it would be reasonable to expect security staff to go through the most rigorous security checks and it may be necessary for the organisation to consider a comprehensive security assessment. Cross functional teams, given the responsibility for the security provision need to understand potential vulnerabilities that can arise in specifying a security provision for their organisation. These typically will include:

- Inflated costs
- Increased staff costs
- Risk or exposure to the organisation
- Not incorporating the cost of maintenance/management
- Inaccessibility to Police and Emergency External Agencies.

Moreover, it is essential that in considering their options, cross functional teams consider a variety of security measures that will deliver your key objectives as well as understanding if the planned security provision conflicts with any other security measure already in place.

4.3. Prequalification and supplier selection

There are many issues to be considered in the prequalification and supplier selection phase. The most critical are detailed below.

- i. Supplier selection is difficult when an organisation is purchasing services such as security provision. Procurement professionals may attempt to quantify the differentiators of a potential supplier that makes them different from the herd. And before any progression is made in this phase procurement professionals need to establish what objectives are to be achieved by acquiring the security services. Do they want an 'Entente Cordial' or an 'Unholy Alliance'? Whichever is decided upon the procurement process needs to be approached with this in mind.

- ii. We have already identified the importance of cross functional teams and it is important to remember that facilities management personnel often administer the security provision for their organisation and it is becoming increasingly important that the prequalification and supplier selection is undertaken with this fact in mind. As with most functional areas within the organisation, facilities management will often have an overarching strategy that will at the very least need to be taken account of.

- iii. There are legal aspects which also need to be considered. A propos the legislative changes within this sector procurement professionals will not only need to trawl the marketplace but also seek advice from organisations such as BSIA and TSI who are the principle agencies within the UK able to offer advice regarding the credentials of a security provider.

- iv. As mentioned above many security providers feel that procurement professionals purchase security based on cost alone. This may be an appropriate methodology if the buying organisations strategic intent is cost leadership and the market conditions suit and the only differentiator being offered by the competition is cost. However, supplier selection and prequalification should be extended beyond the parameters of cost and should feature some of the following:

a. The security provider's company

- Their strategy, vision and objectives
- Their culture, philosophy and policies
- Financial profile
- Range of services
- Track record
- Capacity planning.

b. The Commercial offering

- Supplier's profitability
- Expectations versus requirements
- Quality of service and product
- Knowledge transfer
- Terms & conditions
- Price
- Continuous improvement
- Level of risk.

c. Contract management

- Contract structure and skills of the management team
- Technical knowledge
- Management information
- Supplier development
- Resource availability
- Technical support.

In essence, procurement professionals should be trawling the marketplace 'desperately seeking **SUSAN**'

- **S**uperb supplier
- **U**nconditional trust
- **S**ecurity of supply
- **A**daptable and flexible suppliers
- **N**o surprises!!

Introduction to Purchasing Security

4.4. The Contract

The challenge faced by the parties who are trying to formulate a contract is due to the constant changes that take place within legislation in the UK the EU and further a field. This puts pressure on both procurement and security providers to contribute to their organisation's commercial standing, or in some cases survival. In turn this brings an ever increasing requirement to understand and negotiate terms and conditions of contract that will protect their own organisation's interests and objectives.

When both parties engage in negotiating a contract for security provision careful consideration will need to be given to the clauses used in the contract. The clauses and recommendations shown below can be used as standards known as 'boiler plate' clauses which are embedded in many forms of commercial contract such as distribution agreements and contracts for the supply of goods and services.

These are the additional provisions which usually appear at the end of an agreement. They are not the substantive clauses in a contract such as A sells goods or services to B or the warranties and obligations of the parties. It is important to ensure boiler plate clauses are compatible with the remainder of the contract. Additionally specific legal advice should be taken for individual circumstances.

Generally business is conducted on a goodwill basis, as the provider will be looking for future business and the procurement professional will expect their security requirements to be executed in a prompt and effective manner. As disputes can arise in all manner of ways strict adherence to the contract forms the ground rules with which such disputes can be discussed and resolved. If both parties have failed to establish and agree the terms of the contract that will deal with the resolution of disputes the business transaction for the security provision would be conducted under common law. In a worst cases scenario, default could result in the insolvency or

Fig 2 Table of Boilerplate Clauses

Insolvency & Bankruptcy	Force Majeure
Confidentiality	Intellectual Property
Data Protection	Publicity
Waiver	Termination for Breach
Terms of Payment	Time of the Essence
Notices	Entire Agreement
Dispute Resolution	Assignment and Subcontracting
Statutory Regulations	Health & Safety
Law	No Third Part Rights
Severance	Agency
Environment	Conflicts of Interest
Fraud	Competition Law
Discrimination	Transfer of Undertakings (Protection of Employment) TUPE

bankruptcy of the defaulting party since damages could be unlimited.

Therefore, it is in the interest of both the procurement and the security professional to establish at the very least some basic protection in the eventuality of an un-resolvable dispute or justifiable claim for damages. Ultimately resolution is best achieved when both parties can discuss the problems face to face.

4.5. The Service Level Agreement (SLA)

Service Level Agreements (SLAs) are integral in making relationships with suppliers work, especially outsourcing arrangements such as a security provision. The purpose of the SLA is to define the scope of the security provision, identify performance objectives for the delivery of the security provision, and document the business units and individuals within those business units who are responsible for meeting SLA conditions. In effect, the SLA clarifies the interpersonal and operational working relationships between the client organisation and its security provider. It would be a serious risk to both parties entering into a security provision agreement to not develop an SLA.

"A well dressed buyer goes into a care dealer to order a new car. He gives the car salesman an enormous sum of money and says, "Select the best car you have and deliver it to me next week". The buyer quickly signs a blanket purchase authorisation and leaves, confident that he impressed to the sales person that he expects the best car money can buy. The following week the buyer returns to pick up his car. The salesman greets him and escorts him to his new car. It is a shiny red, factory fresh mini. Agbost, the buyer exclaims, "This is not what I ordered. I paid for the best car money can buy!" The salesperson calmly says, "That is exactly what you have, sir. The mini is fuel efficient, can fit in any parking space, is nimble, and peppy to drive and will get you to your destination as quickly as you could in a larger car, assuming you stay within the speed limit."

Buying security services works in much the same way as in the analogy above. It is the obligation of the procurement professional to specify the exact delivery requirements and the SLA is the right tool for doing this as it avoids ambiguity. Because all relationships are unique, SLA's will differ. The following are recommendations of what should be covered in the SLA:



Introduction to Purchasing Security

- Business objectives and objectives of the SLA
- Procedures for updating the SLA
- Responsibilities of the supplier
- Responsibilities of the client organisation
- Performance reviews: systems, frequency of reviews
- Problem management
- Security management
- Setting priority or severity levels
- Service level incentives and penalties
- Key Performance Indicators or performance metrics.

4.6. Key Performance Indicators (KPIs)

Detailing the correct KPI levels are critical to the success of ensuring that the client organisations expectations are clearly defined and that the security provider understands the standards by which their performance will be appraised. KPIs are unique to each organisation, but should be subject to change during the life of the contract.

Procurement professionals should develop organisation specific KPIs that help enhance the value that a security provision offers. Above all procurement professionals should avoid adopting standard KPIs already developed by other organisations. Procurement professionals can use standard KPIs as a way of benchmarking or base lining not only a current security offering but another organisations security provision. Below are some KPIs that have been used by a variety of organisations to measure or benchmark the performance of a security provider:

a. Documentation

- Management information support, including the monitoring of external data on regional threats and advising on an appropriate course of mitigating actions
- To ensure that compliance information is provided in accordance with your organisations risk management process
- All documentation related to the operation of security at your organisation is correct and up to date at all times eg key register, swipe cards operating instructions for systems, image management control.

b. Customer interfaces

- To ensure that assignment instructions are reviewed with the client organisation on a monthly basis
- Contract manager or deputy is fully empowered to make decisions relating to the operation of the security services including recruiting and removal of staff
- Do all security personnel remain customer focussed at all times?

c. Innovation & improvement

- Submissions of proposals for future security innovation
- Culture, does the security provider drive an improvement culture?
- Remedial actions, does the security provider demonstrate effective remedial action processes, or are there frequent repetition of problems.

d. Skills, competencies & training

- Daily scheduling and reconciliation
- All officers including support officers are correctly trained to perform their duties and are courteous at all times
- Officers including support officers are fully aware of and compliant with procedures within assignment instructions
- Service engineers are trained and qualified to maintain and recommission systems.

e. Service quality

- To ensure that key, access control and CCTV procedures are monitored in accordance with the guidelines laid down in your organisation, including all relevant legislative requirements
- All buildings are opened and locked down in accordance with assignment instructions
- Uniforms must be worn correctly in accordance with assignment instructions
- Faults are attended to appropriately within time limits specified.

f. Commercial management

- All costs are in budget
- Does the security provider proactively liaise with the procurement professional to reduce costs and ensure all cost and efficiency savings targets are either achieved or exceeded before the target dates?
- Can the security provider process claims in a timely manner?
- Are systems designed to remove unnecessary running costs or maintenance?

There are more areas that security can be benchmarked, eg health & safety, installation, commissioning and decommissioning of security equipment, project management and so on. The list is endless; however, it is important to choose those which fit with the objective of the purchase.



Introduction to Purchasing Security

5. Hints & Tips

This section of the document aims to help you plan buying security services for your organisation.

1. Develop a cross functional team. This should be identified through undertaking stakeholder analysis, and requires representation of all the relevant business functions in your organisation.
2. Build a risk profile. This is the responsibility of the cross functional team, it is important to ensure that the risk profile considers the organisational strategy to ensure no misalignment occurs.
3. Procurement professionals will need to undertake a risk analysis that investigates the level of supply risk in the market place and the profit impact within the business (Kraljic 1983).
4. Define your requirements. Do not be so prescriptive in your definition that it stifles any innovation that a security supplier may bring.
5. Try not to place too much onus on your current security provision. Look for a solution that best protects your organisation. It's ok to change things!
6. Make certain that any security suppliers invited to tender have the ACS accreditation or you have satisfied yourself that they meet alternative standards.
7. Ensure that any criterion used to select suppliers extends beyond cost benefit.
8. Make sure that all clauses reflected in the contract are relevant to the security provision being delivered.
9. Pay particular attention to the SLA. It is integral to the success of the delivery of the security provision. Ensure that the SLA covers issues such as: objectives, responsibilities and performance reviews.

10. Ensure that any KPIs chosen are agreed and are both relevant and proportionate to the security provision being delivered.

6. Conclusion

In a recent survey Forrester Research asked 1,900 “decision makers” in North American, European, and Asian Pacific enterprises to prioritise their organisations' major technological requirements for the next decade. In all three regions, upgrading security, specifically its technological aspects emerged as the top priority, emphasising the importance business leaders are placing on ensuring their organisations are protected in what is becoming an increasingly problematic business world (28 per cent of firms cited the initiative as critical).

Respondents from China and Germany/Austria are the most focused on making significant upgrades to their security environment; 43 per cent and 40 per cent of decision-makers in these countries, respectively, rank it as a critical priority. Interestingly, the respondents least likely to see security as job one in 2006 were those from the United Kingdom. Only 14 percent of UK respondents deemed upgrading their security environments a critical priority.

This document intends to provide insight into recent legislative changes within the private security industry and has been written with both the security professional and procurement professional in mind. Both parties will hopefully develop knowledge on what good procurement practice looks like and what considerations need to be taken account of in the provision of a security service for their organisation. If this product enables dialogue between the procurement professional and security professional then it will have achieved its objective.

- i Source: The Security Industry Authority Corporate Update, Summer 2006
- ii Source: Quote from Roy Ayliffe, FCIPS, Director of Professional Practice, CIPS
- iii Source: Quote from Stuart Lowden, Managing Director. Wilson James
- iv Source: Adapted from an IPSERA 2001 conference research paper titled ‘Advancements in the use of a purchasing portfolio approach’ authors; Kees Gelderman, Arjan van Weele
- v Source: Adapted from a research paper titled Strategic Analysis Report by S. Hawkins
- vi Source: Forrester's Security First Look Newsletter dated 6th July 2006

Introduction to Purchasing Security

Useful websites

www.bsia.co.uk
www.the-sia-org.uk
www.cips.org
www.ipsa.org.uk
www.nsi.org.uk
www.ssaib.org
www.securedbydesign.com
www.brecertification.co.uk
www.jsic.org.uk
www.locksmiths.co.uk
www.appss.org.uk

Authors & Acknowledgements

This publication has been co-authored by
Darren Ford, MCIPS & Professor Martin Gill

Darren Ford, MCIPS, is a professionally
qualified Senior Procurement Specialist at the
Chartered Institute of Purchasing & Supply.
Darren can be contacted at
darren.ford@cips.org

Martin Gill, PhD, is Director of Perpetuity
Research and Consultancy International
(PRCI) a spin out company from the
University of Leicester where he is a Professor
of Criminology. He has published widely (12
books and over 100 articles) and has recently
edited the Handbook of Security. He is a
Fellow of The Security Institute, a member of
the Risk and Security Management Forum, the
Company of Security Professionals (and
therefore a Freeman of the City of London), he
is Chair of the ASIS Research Council and an
overseas representative on the ASIS
International Academic Programs Committee.
Martin can be contacted at
m.gill@perpetuitygroup.com

Both authors would like to thank colleagues
and all those who helped to produce this
publication





Introduction to Purchasing Security

Questions & Answers

How do I clearly identify and communicate my security requirements?

Firstly it is essential to undertake a risk assessment and an audit of current security provision to facilitate the development of a clear security strategy. This will then aid the development of the specific requirements that will need to be communicated in the tender document.. It is important that the supplier identifies key questions in the tender document and discusses them with the security provider. who will welcome the opportunities to clarify your priorities. Suppliers often report that some tender documents include lots of questions that look like they apply to a different tender or a separate piece of work; be sure to include only those that are relevant. If you are tendering for security products rather than services then it is especially important to specify exactly what you want the equipment to do. Providers note that sometimes the specification is loose and this enables some suppliers to quote for equipment that will do the job but is not the best available. It is always important to understand what outputs you want from security, some suppliers note that they do not feel P&SM Professionals are always entirely clear. The tender process should enable suppliers to ask questions and offer constructive advice. As one respondent noted:

"There are some (buyers that) are sloppy about buying security. It is not part of their main job, they don't understand security. How many companies say they want CCTV and then go to a supplier and say can I have CCTV please? Many don't understand the benefit of what a good CCTV system can do. It protects your business, your assets, your workforce, reduced staff turnover, reduced insurance."

What are the benefits of using accredited suppliers?

There are many different types of accreditation for the security industry and sometimes it can be difficult to understand what they all mean.. Depending on the accreditation body concerned, these benefits can consist of:-

Accountability, the company is answerable to an organisation regarding its conduct and standards of products and services

Quality, the company has demonstrated that quality products and services are central to its ethos by complying with quality standards via independent inspection

Standards, compliance with, and contribution to, the formation of standards

Viability, the company has demonstrated that it has adequate insurance provision and a sound financial history,

Informed, the company receives timely information on developments in the industry that may affect their clients

Networked, the company has the opportunity to interact with other members and form strategic partnerships,

Assurance, the client receives peace of mind when using an accredited company

Are those who quote the lowest price capable of delivering the contract?

If a quote comes in very low, the buyer must question why. Is the supplier cutting wages, offering fewer benefits or less training? If so this may impact on the supplier's ability to deliver the contract to the quality desired. It is because the client organisation is particularly prestigious and are they prepared to lose profit to get this one job? Or are they simply very efficient and cost effective? If so they probably are capable of delivering the contract adequately.

The key is, when a quote is low, ask why and make an informed decision from there. One procurer interviewed during the research noted:

"We turned down the lowest quote because it was suspiciously low. It was significantly lower than the rest and not sustainable. It was a good call because we later found out they were being sold and just wanted a big portfolio to make them an attractive acquisition."

Should you check what is claimed on the tender response?

It is always advisable to verify any claims made in a tender response document, especially if a supplier is unfamiliar to you,. Non verification of claims made in tender responses can lead to some potential consequences for service levels, cost, quality etc when the information presented is not entirely accurate. The Security Industry Authority has recently introduced an Approved Contractor Scheme, and those companies who are 'approved' are required to maintain minimum standards which may help determine quality.

"Now much depends on who you are up against, this is what really bugs me. If you are up against a credible company, fair enough, but often you have people who cannot do the job but promise the earth to get the contract. If price is the only issue we will never beat them so it is just not worth it. Trouble is clients just will not tell you who you are up against."

How do I manage sanctions as well as incentivising my supplier?

Poor services by the supplier may require sanctions but it is important to remember that some schemes can impact directly on security staff. At the same time exceptional service deserves personal recognition and provides an opportunity to reward accordingly. In manned guarding, linking a bonus to exceptional staff performance can motivate people and generate very positive benefits. However,, problems can and will occur and so it is important that there is a good understanding between both supplier and client so that problems can be addressed speedily and to mutual satisfaction.



Introduction to Purchasing Security

"We don't support penalties. We're here to make partnership work and you don't do that by throwing around penalties. Penalising doesn't help and if it [the partnership] is not working you just have to get rid of them."

How do I use Key performance Indicators - KPIs?

KPIs need to be linked to the value that a security service can bring and how it mitigates the risk, hence the importance of a good risk assessment and clarity about security strategy and objectives. Where you know what you want, it is a good idea to include KPIs in your tender documentation; it can help suppliers to respond more appropriately. There should be a second stage of defining KPIs once the contract has been awarded, this should evolve from joint discussion and should stretch the supplier and be based on achievable activities, that where possible, can be independently measured. It should be considered whether you are using tangible or intangible KPI's – for example; having a full staff complement to meet the performance requirements is tangible; responding in 3 minutes to an alarm is tangible. Intangibles can create grey areas and here Service Level Agreements can be helpful to clarify what is required. Some suppliers noted that P&SM Professionals could helpfully ask what factors were critical to the successful delivery of the contract; it helps to focus the minds of both parties.

Why is an overarching security strategy important?

A security strategy, which may include many aspects of risks to the bottom line, can be quite broad, but its existence is vital for suppliers for at least two reasons. First, suppliers can see how they are expected to contribute to the overall plan as well as identify the scope for complementing other services. Second, it provides the framework within which the buyer can assess the value of the supplier's specific contribution to the overall security objectives and it can help identify any gaps. A lack of a strategy can

result in a patchy and inconsistent service which can be expensive.

How can I determine the budget for security operations?

A good risk assessment and an analysis of how the risk can be mitigated can provide a case for determining the necessary funding of the total security operation.

What are the disadvantages of online auctions for security?

Discussion of this issue generates some forthright opinions. Some providers believe online auctions offer a good way of ensuring that the best price is obtained. On the other hand, others feel that it results in people cutting costs to win the contract without thinking through the impact on service provision. Still others pointed to the fact that effective security depends on partnership and therefore building a rapport via face to face communication is crucial.

How do I see through the sales pitch?

A good tendering process can assist with this. For example in the tender documents some P&SM professionals will require suppliers to go beyond merely stating what services or products they could offer and will often require evidence of their ability to provide a good service in the form of client references. It is also advisable that the P&SM professional should insist on meeting the individual that will become their account manager; they will also benefit from speaking to the person in charge of operations not just the sales staff or the managing director.

How detailed should a tender specification be?

There are at least two schools of thought here. One is that the tighter the specification the easier it is to compare the tender submission from different suppliers. The other is that specification stifles innovation. For example, some companies noted that they wanted to offer the client an alternative to the one specified but there was no opportunity, due to the tight specification. For example:

"The specification may say I want someone here for this many hours is one type. If it is another which says keep the buildings safe from marauders. (this) enables security to come up with alternative solutions, the first one does not."

Suppliers have advocated always including an invitation to offer alternatives. However it is important to think through how you will make use of this information. Employing an independent security advisor is one possibility. Part of the difficulty for suppliers is that they are thwarted from providing innovative suggestions because P&SM Professionals often state they will circulate this information amongst all those who have been invited to tender; no company can afford to give away its secrets.

The aim of this document is to help you understand the complexities involved in the buying of security services. There are a few additional points that may be helpful.

- Ensure that you provide clarity on what your security needs are, what factors and issues you consider the most important and your expectations of your security provider.
- Some companies routinely go out to tender, even when they are happy with a supplier; they use it as a way of benchmarking their costs. However asking other P&SM professionals may be a quick and easy way of getting good data.
- Consider the use of independent consultancies to assess the problem and prepare the tender document and advise you on it throughout. This way you can be sure that you get the proper sort of investment in security, that is proportionate to your threats and your company.
- It is worth noting that suppliers stated that the culture operating in your company has a major impact on the effectiveness of security, as security officers spend most of their time at your place of work.



Introduction to Purchasing Security



THE
CHARTERED INSTITUTE OF
PURCHASING & SUPPLY



Easton House, Easton on the Hill, Stamford, Lincolnshire PE9 3NZ, UK

Tel: +44 (0)1780 756777 • Fax: +44 (0)1780 751610 • Email: info@cips.org • Web: www.cips.org



CHARTERED INSTITUTE OF
PURCHASING & SUPPLY



Paper manufactured from wood fibre
from sustainable forests