MULTINATIONAL INDUSTRIAL SECURITY WORKING GROUP
Document Number 25
2 November 2012

RISK BASED ASSURANCE

1. INTRODUCTION

1.1 Building on work undertaken by Canada[1] on 'Risk based Approach to Industrial Security Inspections and by the Netherlands[2] on the 'Outsourcing of Security inspection and Audits' the MISWG Conference 2010 in Slovenia established Ad Hoc Working Group 6 (AHWG6[3]) to:

*"Examine (on the basis of the outcome of the Canadian and Dutch presentations at MISWG 2010) what **risk based practices** and **measures** are currently being applied or may be adopted by the MISWG participants, faced with decreasing resources and an increasing workload in order to achieve an **acceptable level of assurance** of compliance with national or international industrial security laws and regulations by companies or other economic operators".*

1.2 This remit was agreed to facilitate further consideration of a risk management approach that offered a solution to the growing gap between the growth of industrial security programs and available Government security assurance resources being experienced by some MISWG participants. In these circumstances it is becoming increasingly important that scarce expert Government security resources are directed at those companies/facilities constituting the greatest risk.

1.3 Given the level of debate generated during MISWG 2010, it was considered extremely unlikely there would be a single solution or 'right way' emerging from its activities that would meet all assurance requirements for every participating nation. This assumption was re-enforced during AHWG6 workshop discussions primarily because MISWG participants have different:

- National Security Laws and Regulations
- Understanding concerning what constitutes 'an acceptable level of assurance'.
- Risk appetites and approaches to risk management
- Resource availability/constraints
- Actual requirements – these are dependant on the scale and nature of each nations Defence industrial base and extent to which Contractors are required to receive and handle Classified Information.

[1] See Appendix 1

[2] See Appendix 2

[3] AHWG6 participants - UK (Chair), Australia, Belgium, Canada, Croatia, Finland, France, Germany, Israel, Latvia, Luxembourg, the Netherlands, New Zealand, Slovakia,..

1.4 Therefore, from the outset AHWG6 was clear that its remit was to explore the options available to MISWG participants in seeking continued compliance assurance (including IT inspections) rather than to establish definitive "one-size-fits-all" guidance document.

1.5 It was also clear that its remit did not seek to cover the requirement for an initial Facility Security Clearance (FSC[4]) and covered only Material/Information deemed to be 'Classified'[5].

A full list of Definitions/Glossary of Terms may be found at Appendix 7

2. STATEMENT OF INTENT

2..1 Assurance inspections/audits in the industrial security context are the means by which Government Authorities (e.g. National Security Authorities (NSAs) and/or Designated Security Authorities (DSAs)) ensure that companies contracted to handle/manage classified material/information, abide by the security standards set by the relevant National and International legislation, policies and regulations.

2.2 At the MISWG Conference 2011 in Helsinki, AHWG6 sought MISWG approval to proceed on the basis of a revised statement of intent focusing on the future rather than current assurance practices. AHWG6 work proceeded based on the following:

"Based on the assumption that there can be no definitive/prescriptive outcome, AHWG6 is working towards establishing a forward looking, minimum 'first principles' set of common criteria and a framework of options that participants can use to establish a minimum acceptable level of compliance assurance, which maybe further augmented in accordance with any relevant National Industrial Security Laws and Regulations".

2.3 This document seeks to establish the minimum acceptable 'baseline' requirements to be used by MISWG participants to seek compliance assurance. It is structured around the three basic principles identified in AHWG6 original remit and its statement of intent:

- Compliance Assurance
- Risk Management - Assessment Criteria
- Options for Delivery

[4] As defined in "Industrial Security Clearances for {NATO}[4] contracts - Facility Security Clearances (FSC)". See Appendix 6

[5] As defined in List of Definitions/Glossary at Appendix 7 and includes all sensitive material e.g. that which may be marked as 'Protect'.

2.4 In the absence of any other definitive guidance the paper draws on established and already agreed upon principles and definitions, for example: NATO Definitions. This document is based on the assumption that the initial FSC has been already granted in accordance with national laws and regulations (i.e. the requirement for a site inspection for companies physically safeguarding information on their sites). The guidance is therefore intended to cover the periodic, on-going assurance requirements whilst any FSC clearance remains relevant and extant.

3. ASSURANCE

How assurance is achieved?

3.1 It is a basic audit principle that assurance may be gained through a number of different methods and not solely through a 100% verification or compliance check, e.g. delivered via face-to-face audits/inspections. The level of confidence that maybe gained when a particular review methodology is utilised may vary dependant on the circumstances and the rigour with which it is applied. Recognising that there may be national laws/regulations that mandate 100% face- to-face verification inspections this paper works to establish guidance for the development of practices that may be employed through the appropriate application of a variety of methodologies to achieve assurance which may also include intangible factors e.g. The ability of an experienced security compliance officer to know something is not quite right without knowing why.

What level of assurance is considered acceptable?

3.2 It is very difficult to be prescriptive about what is considered ‘acceptable’ assurance because this would depend the specific requirements of individual participating nations (which may be mandated by national laws or regulations) and/or their individual Risk Appetite, i.e. the level of risk that they are prepared to accept. The level at which assurance is considered ‘acceptable’ may also be influenced by the context in which risk is considered. e.g. where a Contractor is managing/handling Foreign Classified Material.

3.3 Whilst accepting that it is difficult to be prescriptive, this document sets forth a minimum set of compliance assurance activities/criteria, which may be used as baseline requirement for Authorities when considering when and how to seek assurance. This baseline requirement may be further augmented/amended by participant nations to meet their own individual assurance requirements, and any relevant national industrial security laws and/or regulations.

Minimum Assurance Requirements

3.4 The following principles are considered to be the assumptions from which the AHWG6 worked:

3.4.1 Overall responsibility for assurance rests with the Government Authority (i.e. NSA/DSA (or equivalent) regardless of the methodology that is used to establish the assurance. - **The Government must retain the ultimate oversight/control to satisfy that responsibility.**

3.4.2 There is a requirement for an initial on-site Facility Security Clearance (FSC)[6] inspection, that establishes a Contractor (and its facilities) is capable of handling and protecting Classified Information/Material – **An 'on-site' compliance inspection is required for <u>all new</u> FSC facilities.**

3.4.3 There is requirement for the Authority to establish a formal compliance assurance regime to ensure that the Contractor (and its facilities) can continue to satisfy/meet the mandatory security requirements for handling and protecting Classified Information/Material through the life of the relevant contract(s)/programmes. **Assurance activities must not be 'left to chance' or based on an 'ad-hoc' approach.**

3.5 As a minimum, the Authority's formal compliance regime must include the following:

3.5.1 An accepted and documented Risk Assessment and Risk Management process – i.e. a process that is transparent, recognised and adhered to by Security Authority Stakeholders

3.5.2 A requirement for some form of legally/contractually binding agreement by Contractor to continue to ensure compliance after the initial FSC has been granted.

3.5.3 A requirement to consider what addition measures may be required in order to help ensure the protection of the more sensitive or highly classified information/material – e.g. there be a requirement to place additional restrictions/exclusions on companies/facilities that handle specific levels of Classified Information/Material (e.g. TOP SECRET)

3.5.4 A requirement that the Government body responsible for assurance (e.g. NSA/DSA) reserves the right to undertake periodic 'on site' inspections – this should be included as part of the process or methodology.

[6] As defined in "Industrial Security Clearances for {NATO}[6] contracts - Facility Security Clearances (FSC)". See Appendix 6

3.5.5 A formal identification of roles and responsibilities[7] within the assurance process - This should be used to establish/recognise the key players and their respective roles in the process, for example:

- Government (NSA/DSA) - Overall responsibility (planning and oversight) owner, FSC Authority, inspection sponsor.
- Government institutions - Classified contract sponsor.
- Legal entity (private) – Contractor.
- Inspection entity – Auditor (maybe Internal/Outsourced).

3.5.6 In this construct the inspection sponsor and inspector/auditor could be either the same or different institution. This should help address to any process issues for participants that have different designated authorities within the Government sector for policy planning and inspections.

4. RISK MANAGEMENT (Risk Based Practices and Models)

4.1 Whilst it is difficult to be prescriptive about what would constitute an acceptable level of assurance, the determination of what best 'fits' for each participating nation should be based on due consideration of what is required and what can be achieved.

4.2 In an era where government resources are shrinking, it is necessary to focus assurance efforts on those areas of greatest need, based on an understanding of the associated risks, rather than to struggle to maintain a 100% 'on-site' inspection regime which may serve to remove a sense of responsibility from the Contractor while serving as nothing more than a 'tick box' exercise that is of no added value to the Authority or the Contractor.

Risk Assessment

4.3 There are numerous Risk Management models and methodologies, most of which are widely available commercially. Many are based on a similar process to identify and mitigate risks and each has its own merits/drawbacks.

4.4 However, whilst the choice of methodology maybe up to individual Authorities, the key premise that must applied is that: a defined methodology is employed, that is transparent, documented, and repeatable with the same or similar results and is able to withstand audit.

4.5 In order to assist Authorities with the formulation of a compliance assurance regime based on Risk Management (practices and measures) the

[7] See Definitions/Glossary of Terms – see Appendix 7

following has been developed as an example of a Risk Management Model[8] for the prioritization of companies requiring security assurance audits and which may assist in the determination of Assurance Inspection requirements.

Example – Risk Management Model

4.6 The example risk assessment model is based around an assessment tool (Annex A) and assessment model (Annex B) which have been developed to identify assess the relative risk level, against a list of common criteria, sub-criteria and further considerations, of companies requiring renewal inspections. The criteria and sub – criteria against which assessments are to be made are:

4.6.1 Organisation/Structure
- Size
- Complexity
- Location
- Infrastructure
- Changes to Ownership/Senior Management
- Type of Organisation

4.6.2 Classified Material, Asset/Information
- Quantity/Volume
- Attractiveness of Asset
- Level of Classification
- Level and type of FSC held
- Presence of Foreign Classified Material
- 'Special Projects'
- CIS & New Technology

4.6.3 History of Compliance
- Type of Incidents
- Number of Incidents
- Reporting History
- Application of Remedial Recommendations

4.6.4 Security Culture
- Previous Experience of Company
- Company's Overall Attitude to Risk
- Application and compliance with Security Processes
- Experience/Effectiveness of the Company Security Officer

4.6.5 Overarching Threats

[8] Model based on the Canadian Risk Management Model, as outlined at MISWG 2010 . See Appendix 1

- Current Risk/Threat Assessment
- Cyber Threat

Consideration/Assessment Tool

4.7 The example consideration/assessment tool has been developed to assist NSA/DSAs, as the Authority, to make an assessment of risk, i.e. what is the assessed level of risk associated with the Classified Information/Material, as held by a commercial organisation, in respect of post FSC assurance and to be used in support of the requirement /assessment model.

4.8 The tool allows the assessor to insert narrative comment and allocate an initial assessment – High/Medium/Low against each of the sub-criteria and associated considerations. This may then be consolidated into an overall assessment of each criterion and may be input to the Overall Assurance Risk Assessment in respect of the Company/Facility that is the subject of the Assessment.

4.9 When using this assessment tool it should be remembered that it is the responsibility of the Security Authority to ensure that the assessor/inspector has the relevant training and experience to competently discharge their responsibilities. This is likely to include consideration of the potential impact of a consolidation of the individual criteria assessments and the need to apply an element of judgement when considering the relative impact of any or all of the relevant risk factors. Any assessment of the current position should also reflect any changes and/or ongoing concerns since last assurance visit and/or granting the FSC.

4.10 This type of model is predicated on a level of cooperation between the many stakeholders within the Industrial security context which may not currently be in place. NSA/DSA's may need to institute new ways of working, process or networks (IT or interpersonal) in order to gain access to all the information that maybe required.

Risk Assessment Model

4.10 The Assessment tool at Annex B is designed to be used in conjunction with the document – "DETERMINING THE REQUIREMENT/RISK ASSESSMENT MODEL".

4.11 The model provides the assessor with a set of potential scenario's that identifies examples of potential High/Medium/Low Risk Factors that could be considered when assessing Contractors against individual Criteria and Sub-Criteria. The model is intended to be used as a guide to enable the assessor/inspector to make a more objective, defensible judgement regarding

the potential risks, it should not be considered to be a definitive articulation of all risk factors. As with the assessment tool it is the responsibility of the Security Authority's assessor to apply an element of informed judgement when considering the potential relevance and impact of any or all of the risk factors.

4.12 The model, as described, does not include any requirement for the criteria/sub-criteria to be factored/weighted. Any assessment of which criteria may or may not be considered to be more important or of greater relevance to the overall assurance assessment should remain a judgement that is the responsibility of the Security Authority, in accordance with any relevant National Industrial Security Laws, Policies and Regulations. If required the Assessment Tool and Overall Risk Assessment form maybe adapted to include factor/weighting.

4.13 The model assumes that the requirement for a physical inspection will be set at periodic intervals, by the Security Authority, in accordance with relevant National Industrial Security Laws, Policies and Regulations. Again the model maybe adapted to include a required frequency and/or timescale for inspection/review.

5. OPTIONS FOR DELIVERY OF ASSURANCE

5.1 Once an assessment has been completed it remains the responsibility of the Security Authority to determine what assurance action is required and the frequency with which future assessments should be undertaken.

5.2 It is also for the Security Authority to determine the instances when a visit/inspection/review is an absolute requirement however, additional/alternative security action is likely to be required where the risks are considered unacceptable to the authority or where an incident has been confirmed as a Security Breach

5.3 It has been accepted that, for some MISWG participants at least, there is a growing gap between the volume of industrial security programs and available assurance resources. In these circumstances it is becoming increasingly important that scarce expert Government security resources are directed at those companies /facilities constituting the greatest risk. Therefore, having taken a risk based approach to the assessment for a security assurance, Security Authorities may wish to further consider the options available to them for the actual delivery of the Assurance capability.

5.4 The following options have been offered by participating Authorities as examples of alternative methodologies, i.e. to conducting an 'on-site' inspection in every instance (post FSC) where compliance assurance is sought. Each option is based on the experience of the Security Authority of that country,

identifies the methodology, benefits/advantages and risks/disadvantage as well as examples of when it might be appropriate to use. The options considered are:

5.4.2 Risk Based Security Inspections – Canada – Appendix 1

5.4.3 Sourcing – Netherlands & Finland – Appendix 2

5.4.4 Controlled Self Assessment – UK - Appendix 3

5.4.5 Industrial Security Report – Germany – Appendix 4

5.4.6 Private Companies & Contractors – Security Division – Israel Appendix 5

5.5 This list is not exhaustive and the various options are not intended to be mutually exclusive. Authorities may well decide to adopt a different approach or even a hybrid of the options detailed in this paper.

6. CONCLUSION

6.1 It is very difficult to be prescriptive about what is considered an 'acceptable' level of assurance or to determine what would be an appropriate methodology for the assessment of risk and delivery of assurance activities, as this is dependant the specific requirements of individual participating nations, which may be mandated by National Laws or regulations. This paper does not seek to create a definitive model for what risks may be considered acceptable/unacceptable, however, it does define the minimum requirements for any risk managed system which would permit ongoing confidence in an industrial security programme.

6.2 The paper sets out some common principles of risk assessment which are intended to assist Security Authorities in the prioritisation of their assurance oversight/inspection cycle and explores some of the options available to them for delivery, other than the requirement to make an 'on site' renewal inspection in every instance.

6.3 It remains the responsibility of the Security Authority to determine what assurance action is required, how it should be delivered and the frequency with which future assessments should be undertaken. However, the key premise must be that the authority has established a formal compliance assurance regime to ensure that the Contractor (and its facilities) can continue to satisfy/meet the required security requirements for handling and protecting Classified Information/Material through the life of the relevant contract(s) programmes. This should include a defined methodology for the assessment of risk that is transparent, documented and available for audit scrutiny.

RISK BASED ASSURANCE
CONSIDERATIONS/ASSESSMENT TOOL – EXAMPLE DOCUMENT

This example of a consideration/assessment document has been developed to assist NSA/DSAs, as the Security Authority, to make an assessment of risk, i.e. what is the assessed level of risk associated with the Classified Material, as held by a commercial organisation, in respect of Post FSC assurance and to be used in support of the requirement /assessment model.

When using this assessment it remains the responsibility of the Security Authority's assessor/inspector to consider the potential impact of a consolidation of the individual criteria assessments and to apply an element of judgement when considering the relative impact of any or all of the risk factors.

Any assessment of the current position should also consider any changes and/or ongoing concerns since last assurance visit and/or the granting of the FSC.

This document is designed to be used in conjunction with AHWG6 Document 2 – "DETERMINING THE REQUIREMENT/RISK ASSESSMENT MODEL".

Criteria	Sub Criteria	Considerations	Mitigations/Comment	Low	Med	High
Organisation/Structure *Does the overall organisation or structure give cause for concern?*	Size	**Consider the overall size of the company in relation to the other assessment criteria.** - Does this have any significance in relation to security? For example: A larger company may be more complex and have many Classified projects but it also may have a more developed security culture if normally participating in large Classified projects. Conversely a smaller company may have a simpler structure and have fewer Classified projects but it may be inexperienced in Security.				
	Complexity	**Consider how the complexity of the Company's business might impact on security**: - What is the span/diversity of its activities and how is this managed? - Does the complexity of its business require different systems of security control? - Is there a requirement for 'cross				

RISK BASED ASSURANCE

CONSIDERATIONS/ASSESSMENT TOOL – EXAMPLE DOCUMENT

Criteria	Sub Criteria	Considerations	Mitigations/Comment	Low	Med	High
		discipline' working? - What is the relationship and balance of influence of the various divisions within the company? - Does the company sub contract?				
	Location	**Consider whether there are any risks associated with the location of the Company/FSC facility:** - Is activity split over more than one location? - Is activity undertaken at a Government 'secure' site? - Is the facility/site in a remote location? - Is facility located in an industrial (or even residential) area? - What is the general security situation of the area – incidence of break ins/vandalism etc.? - Is the organisation re-locating?				
	Infrastructure	**Consider the general infrastructure of the organisation:** - Is it located in a multi-tenanted building? - Is it own property or rented? - Who are the 'neighbours'? - Have there been any renovations/upgrades or building moves? - Any new developments or re-organisation? - Have any services/activities been outsourced?				
	Changes to Ownership/Senior	**Consider whether there have been any changes of ownership since the last**				

RISK BASED ASSURANCE

CONSIDERATIONS/ASSESSMENT TOOL – EXAMPLE DOCUMENT

Criteria	Sub Criteria	Considerations	Mitigations/Comment	Low	Med	High
	Management	**assurance assessment or when FSC was completed:** - Changes to ownership - Changes to senior management/board structure – new member? - Subject to merger or acquisition activity? - Has there been any change to the balance of influence? - Changes to FOCI? Also consider whether any other changes in circumstances need to be considered: - Is the organisation subject to merger or acquisition activity? - Has there been any changes to control/influence associated with any foreign ownership? - Is the organisation itself re-structuring e.g. Downsizing?				
	Type of Organisation	**Consider whether the type of organisation has any potential to impact on security:** - Service or manufacturer? - Multinational? - Is the company considered to be financially stable? - Is it involved in any collaborative programmes/projects? (NB. these might be National or International) - Is it a Joint Venture? (NB. these might be National or International) - Niche Supplier? - Small/Medium Enterprise or 'one				

RISK BASED ASSURANCE

CONSIDERATIONS/ASSESSMENT TOOL – EXAMPLE DOCUMENT

Criteria	Sub Criteria	Considerations	Mitigations/Comment	Low	Med	High
		man band'? - What is the main business focus – Govt or Commercial - Market specific e.g. Defence/Civil? - Is the organisation involved in any Joint Ventures or Collaborative projects? (NB these could be National and/or International)				
The Consolidated Assessment for Organisation/Structure Criteria =						
Classified Material Asset/Information – managed, held, processed *What is the potential impact of these risks in relation to the sensitivity of the material involved?*	Quantity/Volume	**Consider the quantity/volume of Classified material**: - Level of assets - how many - Value - may be linked to level of classification and attractiveness of asset. - Volume to Value ratio e.g. large numbers – low value.				
	Attractiveness of Asset	**Consider the attractiveness of the asset/material concerned:** - Its value - Its capability - Usefulness to others - To provide access to something else - Could the material be considered of particular value? e.g. a strategic or unique product?				
	Level of Classification	**Consider the highest level of Classified Material:** - What is the maximum level of Classified Information/Material? The inherent risk level maybe greater the higher the level of classification. However, the risk level may also be linked to the volume and value of the material held				

RISK BASED ASSURANCE

CONSIDERATIONS/ASSESSMENT TOOL – EXAMPLE DOCUMENT

Criteria	Sub Criteria	Considerations	Mitigations/Comment	Low	Med	High
		(e.g. is one Secret any more than twenty Confidential?) May also be linked to level and type of FSC. - Does the level of classified material match the FSC level and type?				
	Level and type of FSC held	**Consider the original Facility Security Clearance (FSC):** - Was there anything of concern when FSC was granted? - To what level was FSC granted? - What is the type of FSC? - Does the level of material held match the level and type of FSC? - When does FSC expire? - When was facility last visited? - What was the outcome of the last assurance visit? - Are there any ongoing concerns? - Is this facility a 'new' FSC? - Is there a requirement for CIS Accreditation? - Is this still valid?				
	Presence of Foreign Classified Material	**Consider the existence/presence of Foreign Classified Information/Material:** - Is material jointly 'owned'? - Is material incorporated into other item/material? - Is material managed on behalf of another nation? - Are there bi-lateral/multi-lateral agreements/arrangements in place? - Is there any awareness that foreign Classified Information/Material may require additional security				

RISK BASED ASSURANCE

CONSIDERATIONS/ASSESSMENT TOOL – EXAMPLE DOCUMENT

Criteria	Sub Criteria	Considerations	Mitigations/Comment	Low	Med	High
		considerations? - Is the material held/managed as part of collaborative or Joint Venture activity? - What additional requirements maybe in place?				
	'Special Projects'	**Consider whether the organisation is involved in any 'special' projects**: - Do these require additional security considerations, - Do they represent an increased security risk? - Are there any additional requirements/levels of approval required? e.g. Exhibitions/public events?				
	CIS & New Technology	**Consider the impact CIS/technology has on security, e.g. is this a highly IS dependant organisation?** - Are CIS appropriately accredited for level of material being processed? - What is the system architecture – open/closed? - Are the technical/physical security measures require in place and are they up to date?				
The Consolidated Assessment for Classified Material/Assets/Information Criteria =						
History of Compliance *Does the compliance history of the company/organisation give any cause for concern?* *This is likely to be a key deciding factor in whether or*	Type of Incidents	**Consider the severity/type of incidents that have/may have occurred since the FSC was granted or the last assurance assessment.** - How serious are the consequences/impact of any incidents? o Potential Impact				

RISK BASED ASSURANCE

CONSIDERATIONS/ASSESSMENT TOOL – EXAMPLE DOCUMENT

Criteria	Sub Criteria	Considerations	Mitigations/Comment	Low	Med	High
not an assurance visit is necessary.		o Actual impact - Any legal implications? - Involvement of other Govt/Govt Agencies? Clearly anything more than a few 'minor' incidents would suggest that a greater level of Assurance is required.				
	Number of Incidents	**Consider the number and frequency of incidents that have occurred since last review**: - How many incidents? - What is the frequency of incidents? - Seriousness of incident (in relation to frequency) - Is there reason to believe that similar incidents have occurred in the past/are repeated? Should be considered together with the type of incidents, the reporting history and its approach to the application of remedial action.				
	Reporting History	**Consider the reporting history of the company**: - Are incidents reported promptly? - Is there reason to believe that notification reporting of incidents has been withheld? - Does company/organisation co-operate willingly with any investigations?				
	Application of Remedial Recommendations	**Consider the company approach/willingness to implement remedial recommendations/actions**.				

RISK BASED ASSURANCE

CONSIDERATIONS/ASSESSMENT TOOL – EXAMPLE DOCUMENT

Criteria	Sub Criteria	Considerations	Mitigations/Comment	Low	Med	High
		- Does the company/organisation implement remedial recommendations promptly and fully? - Are remedial actions fully implemented or perfunctory? - Are they pro-active in suggesting/identifying remedial actions themselves? - Is the company willing to share audit findings/recommendations? NB. these may have arisen from previous reviews and/or investigation, and may have been conducted by other audit bodies.				
The Consolidated Assessment for Compliance History Criteria =						
Security Culture *What is the overall perception of the company's security culture?* *This should include an assessment of the overall management control system.*	Previous Experience of Company	**Consider the previous experience of the company with regard to security and assurance:** - What has the relationship been like – good/poor? - Is experience of other areas of relevance e.g. Commercial/Procurement team? - Poor track record of compliance - Asks questions they might be expected to know the answer to – 'silly questions' - Is this the first assurance consideration since granting an FSC?				
	Company's overall attitude to Risk	**Consider the company's overall attitude to risk:** - What is the company overall (not				

RISK BASED ASSURANCE

CONSIDERATIONS/ASSESSMENT TOOL – EXAMPLE DOCUMENT

Criteria	Sub Criteria	Considerations	Mitigations/Comment	Low	Med	High
		just security) risk appetite? - Is there a general acceptance that risk needs to be managed? - Does the company appear to be prepared to accept risk that you consider high or inappropriate? - Are risks actively managed or do things seem to 'just happen'.				
	Application and compliance with Security Processes	**Consider the organisations application and compliance with prescribed/required (and own) security processes:** - Is there a 'published' security process/ procedures? - When was this last updated? - Who manages the security for the organisation – internal or external/changes - last FSC assessment? - Any changes to the provision of security? - What is the size and structure of the security organisation? Is it proportionate to the level and volume of Classified Material? - How many Personal security clearances are held and what is the ratio of cleared to non-cleared? - What is the ratio of cleared personnel in relation to Classified Material? - Is the security process well known to all employees? - Has company instigated security and awareness programme? - Is there a 'controlled' visitor				

RISK BASED ASSURANCE

CONSIDERATIONS/ASSESSMENT TOOL – EXAMPLE DOCUMENT

Criteria	Sub Criteria	Considerations	Mitigations/Comment	Low	Med	High
		processing system? - How are foreign visits managed? e.g. is there frequent access to areas where Classified Material held/managed?				
	Experience/Effectiveness of the Facility Security Officer	**Consider the experience of the company Facility Security Officer (FSO)**: - How long has the FSO been in post? - What previous experience does FSO have? - Does FSO or should FSO hold any professional security qualifications? - Is there a relationship of trust? - Is FSO pro-active in the management of security within the organisation? - Does FSO have a good understanding of security issues within the company? E.g. where classified information resides, how it is exchanged etc. - Is FSO generally co-operative with the Authority regarding security? - Does FSO have Board support? - Does the FSO have a role in the change management process?				
The Consolidated Assessment for Security Culture Criteria =						
Overarching Threats *What are the overarching risks to security, in relation to wider business activities – what is the current Threat Assessment*?	Current Risk/Threat Assessment	**Consider whether there are any particular (national security) risks/threats associated with the company, its location, nature of business etc.** - Is the material considered particularly attractive/vulnerable/valuable?				

RISK BASED ASSURANCE
CONSIDERATIONS/ASSESSMENT TOOL – EXAMPLE DOCUMENT

Criteria	Sub Criteria	Considerations	Mitigations/Comment	Low	Med	High
		- Is there a particular general security threat that would suggest that there is an increased risk? - What is the company media profile?				
	Cyber Threat	**Consider whether there is a particular concern regarding Cyber**: Does this aspect present any additional concerns? - Nature of business more susceptible to Cyber threat? - Is there classified material on open/partially accessible network? - Complex interfaces with other systems/ - Links to Govt systems/critical infrastructure? - Links to Open systems - Is security accreditation still extant/valid? - Are technical; and physical protective measures up to date?				
The Consolidated Assessment for Overarching Threat Criteria =						

RISK BASED ASSURANCE
CONSIDERATIONS/ASSESSMENT TOOL – EXAMPLE DOCUMENT

OVERALL ASSURANCE RISK ASSESSMENT IN RESPECT OF COMPANY/FACILITY [XXX]:

Once an assessment has been completed it remains the responsibility of the Security Authority to determine what Assurance action is required and the frequency with which future assessments should be undertaken. Examples of some of the Assurance options that may be considered can be found at Appendices 1 – 5 of MISWG document on Risk Based Assurance.

Additional/alternative security action is likely to be required where risks are considered unacceptable to the authority or where an incident has been confirmed as a Security Breach.

CRITERIA	CONSOLIDATED RISK ASSESSMENT			COMMENT
	Low	Medium	High	
Organisation/Structure				
Classified Material				
Security Culture				
Compliance History				
Overarching Threat				
Overall Assurance Assessment =				

Annex B

RISK BASED ASSURANCE
DETERMINING THE REQUIREMENT/RISK ASSESSMENT MODEL – EXAMPLE DOCUMENT

This risk assessment model has been developed to assist NSAs/DSAs, as the Security Authority, to make an assessment of risk in respect of Post FSC assurance. Any risk assessment should consider current position and any changes/ongoing concerns since last assurance visit and/or granting of the FSC.

*The assessment of the potential seriousness of risks as identified in this model should not be considered as definitive/absolute and the examples used should not be considered mutually exclusive. This model is designed to be used in conjunction with the "*CONSIDERATIONS/ASSESSMENT TOOL".

Criteria	Sub Criteria	Potential 'Low Risk' Factors	Potential 'Med Risk' Factors	Potential 'High Risk' Factors
Organisation/Structure *Does the overall organisation or structure give cause for concern?*	Size Complexity Location Infrastructure Changes to Ownership/ Senior Management Type of Organisation	- 'Simple' organisation - Single business focus - Stable organisation - No changes of ownership - No changes of structure or operations - No change to organisation/structure since previous assurance/FSC	- Small & Medium Organisation - No significant changes of ownership (e.g. No change to Board majority) - No strategic changes of operations	- Large complex, multi-disciplined organisation - Undertaking new business/activity interest - Location of facility (non-govt or 'at risk' site) - Changes to ownership (Frequent or not notified) - Changes to operations (e.g. diversification) - Significant re-structuring or re-location (e.g. Downsizing)
Classified Material – Asset/Information - managed, held, processed *What are the risks associated with the Classification material- what are the sensitivities involved?*	Quantity/Volume Attractiveness of Asset Level of Classification Level and type of FSC held Presence of Foreign Classified Material 'Special Projects' CIS/Technology	- No foreign Classified Material - Low volume Classified Material - Low Level of sensitivity - No specific threat - FSC matches level of Classified Material - No CIS	- Small volume of Foreign Classified Material - Medium volume of Classified Material - Moderate level of Sensitivity al - Level of FSC exceeds that required for sensitivity of Classified Holdings - Additional authorisation required for special projects (e.g. large public events/exhibition) - Small & Non Inter-connected CIS	- Presence of Foreign Classified Material - High level and/or high volumes of Classified Material - Existence of a specific threat – to material and to the company (perhaps for what it does). - FSC doesn't match value/sensitivity of assets held - Additional authorisation required for special projects (e.g. large public events/exhibitions - Large and/or Inter-connected CIS - Classified Information is held/processed on 'open' IS

Annex B

RISK BASED ASSURANCE
DETERMINING THE REQUIREMENT/RISK ASSESSMENT MODEL – EXAMPLE DOCUMENT

Criteria	Sub Criteria	Potential 'Low Risk' Factors	Potential 'Med Risk' Factors	Potential 'High Risk' Factors
History of Compliance *Does the compliance history of the company/organisation give any cause for concern?* *This is likely to be a key deciding factor in whether or not an assurance visit is necessary.*	Type of Incidents Number of Incidents Reporting History Application of Remedial Recommendations	- No incidents - Minor issues dealt with promptly - Company generated improvement actions - Promptly reports security incidents - No ongoing concerns from previous assurance visit or FSC	- Relatively low level severity and frequency of incidents - Company has co-operated fully in investigations - Any previous remedial actions have been fully implemented - No ongoing concerns from previous assurance visit or FSC	- Confirmed Breach - Severity of Incidents - Frequent and/or Multiple Incidents - Reluctance/delay reporting incidents - Company has withheld evidence regarding incidents - Reticence to implement remedial actions
Security Culture *What is the overall perception of the company's security culture?* *This should include an assessment of the overall management control system.*	Previous Experience of Company Company's overall attitude to Risk Application and compliance with Security Process Experience/Effectiveness of the Company Facility Security Officer	- Fully implemented process/system in place - Confidence/trusted Company Facility Security Officer - Previous experience of company is very good - Company has balanced attitude to risk - Company has provided content of Security & processes	- Procedures not fully implemented - Minor/Non-compliance - Limited training or effectiveness of Facility Security Officer - Limited Board support - Implement security awareness process that are not fully applicable to work performed	- Poorly implemented security process/system, - Overall blasé attitude to risk i.e. high tolerance of risk; risk ignorant. - Lack of confidence/trust in company Facility Security Officer - Poor previous experience of Company security - Company not provided evidence of implementation of security and/or awareness
Overarching Threat *What are the overarching risks to security, in relation to wider business activities – what is the current Threat Assessment*?	Current Risk/Threat Assessment	- No particular threat to material held	- Valuable asset - Vulnerable to potential threat but impact assess as moderate.	- Particularly valuable and/or sensitive material/asset - Existence of known threat - Particularly vulnerable to threat.
	Cyber Threat	- No interface/links with Govt system and/or infrastructure - No History of Cyber problems	- Links/interface with Govt Systems and/or infrastructure - Business not particularly susceptible to Cyber attack	- Nature of business makes company susceptible to Cyber attack - History of Cyber problems - Links/interface with critical Govt Systems and/or infrastructure

Appendix 1

RISK BASED APPROACH TO INSPECTIONS - CANADA

Introduction

1. At the annual MISWG in 2009, Canada sponsored a discussion paper on a "risk-based" approach to inspections for consideration by the MISWG in 2010. Inspections in the industrial security context are the means by which governments ensure that registered companies abide by the security standards set by the relevant domestic legislation, policies and international security organizations. The traditional approach to such inspections has been to have a set schedule of site inspections for all companies holding sensitive[9] Government information.

2. Since MISWG 2010 Canada has continued to develop its risk management approach to inspections for Industrial Security. In Canada, company inspections are conducted by two separate programs: the Controlled Goods Program and the Canadian Industrial Security Program as described below:

The Controlled Goods Program (CGP)

3. Registration in the Controlled Goods Program is required in order for a company/individual to examine, possess or transfer controlled goods in Canada. Temporary workers and foreign visitors are eligible to apply for exemption from registration only if a registered person submits an application on their behalf. Registration of a person is valid for a period of up to 5 years after which the company/individual must renew their application. There are approximately 3,900 (4,600 sites) registered persons in the program and the numbers are growing at a rate of between 3% - 5% per year.

4. Controlled Goods include certain sensitive (but not classified) items on the Canadian Export Controls List:

- Group 2: Automatic weapons, firearms, ammunition, bombs, fighter jets, tanks, missiles, chemicals, explosives, etc.
- Group 5 (item 5504): Global navigation satellite systems, ground control stations, and nuclear weapons design and testing equipment
- Group 6: Missile technology

5. The *Defence Production Act* makes provision for inspectors, on behalf of the Minister, to enter and to inspect any place, require the attendance of and

[9] Sensitive information in the Canadian context refers to both Classified and Protected information, as well as information included on the Canadian Export Control List..

question any person who will be able to assist in the inspection, request to see documents, remove and detain controlled goods and require that any remedial measures considered appropriate are taken. An inspector may be accompanied by any other person chosen by the inspector. The main goal of an inspection is to ensure that there are no transfers of controlled goods to non-registered parties. Since its inception in 2001, approximately 8,312 compliance inspections have been conducted overall (Approx. 1,200 inspections conducted every year).

6. The Controlled Goods Program has developed a risk management approach to inspections. The approach is based on the following factors:

- Business Category (Size of the enterprise, whether controlled goods are on site, how many employees examine, possess or transfer controlled goods)
- Corporate Structure and Ownership (foreign ownership, complexity of structure)
- Company history (number of security breaches, level of compliance, past bankruptcy, etc.)
- Standing in the Canadian Industrial Security Program (is business in default, does it fulfilled the procedures of the program, are there incidents of non-compliance)
- Visit History (does it receive visits from people from certain (risky) countries or visits from non-NATO countries, does it or does it not submit information to the CGP in a timely manner)
- Temporary Worker History (does it employ temporary workers, how many exemptions has it applied for, does it provide the information within the prescribed period, is it compliant)
- Risk Posed by Controlled Goods (what groups of items is the company dealing with?)

7. For each factor, the company/individual receives a score from 1-5 points. The company/individual is then given a total overall score. Based on the score, the company/individual is given an overall rating of low, medium, high, or immediate risk level. There is a corresponding schedule for inspections for each risk level.

8. The risk based approach is currently used for the renewal inspections only. All new registered persons regardless of their risk level are inspected within 64 working days of registration.

Enhanced Security Strategy

9. The implementation of the Enhanced Security Strategy (ESS) did not bring any changes to the inspection risk matrix presented to MISWG in September 2010. However, the new strategy resulted in a number of changes in the conduct of security assessments with the objective to reduce the risk of illegal transfers of controlled goods.

10. Under ESS, Designated Officials are required to conduct security assessments of Directors, Officers and employees accessing controlled goods and Authorized Individuals not accessing controlled goods using a newly developed risk matrix. Those exceeding the risk threshold are sent to the Controlled Goods Directorate for further assessment through security and intelligence partners.

11. Designated Official appointed by the registrant should be someone with sufficient authority, responsibility and integrity within the organization to adequately conduct security assessments.

12. The Controlled Goods Directorate is responsible to security assess owners with more than 20% ownership, Authorized Individuals accessing controlled goods, Designated Officials, foreign students, foreign temporary workers and foreign visitors.

13. The information to be verified and assessed is:

- Biographical and identification;
- Residential;
- Employment;
- Educational;
- Travel History;
- Financial;
- Criminal History;
- Personal References; and
- Significant and meaningful associations.

14. A Security Assessment Application can be denied/granted on the basis of honesty, reliability and trustworthiness and that a person poses a risk of transferring controlled goods to an unauthorized person. A positive security assessment is valid for a period of five years. A security assessment can be reviewed at any time upon receiving new information. Any records collected during the conduct of a security assessment can be verified by a Controlled Goods Inspector.

The Canadian Industrial Security Program (ISP)

15. Based on the positive experience in the Controlled Goods Program, attention then turned to the development of a risk management approach to inspections for the Canadian Industrial Security Program. Registration in the program is required for a company to have access to Protected and Classified Information, NATO information and other foreign origin assets for the purposes of contracting. The program also conducts personnel security clearances. In terms of the number of companies registered in the ISP, there are over 13,000

companies registered for contracts accessing both Protected and Classified information. Physical inspections by a Field Industrial Security Officer (FISO) only take place if the company has a Document Safeguarding Capability (DSC) requirement or Information Technology (IT) processing, but are required at both the Protected and Classified levels. Approximately 31% of companies registered in the Industrial Security Program have DSC or IT requirements.

16. Review / Audit of companies in the Canadian Industrial Security Directorate are conducted based on the following level of security assessment:

- Designated Organization Screening (DOS): This is the standard required for access to Canada's Protected Information. Organizational Review/Audit by the Registration Division takes place every three years. (For companies holding Protected A, the lowest level of sensitive information, review/audit may take place by phone.); and

- Facility Security Clearance (FSC): This is the standard for Classified Information. Organizational Review/Audit by the Registration Division takes place every year for Top Secret FSC and every second year for Secret FSC.

Inspection and Investigation Division

17. Physical Security site inspections are conducted for sites that have a DSC requirement and Information Technology (IT) security inspections are conducted for sites that have an IT security requirement.

18. In respect to renewal site (DSC) inspections companies are only inspected if they have or will be awarded a contract. These inspections are triggered based on a predetermined schedule defined by the level of classification or designation of material being stored or treated by a company. Companies treating higher levels of classification or foreign information are identified for a more frequent cycle of inspections. At present there are over 1,000 inspections carried out every year across Canada.

19. Since MISWG Conference 2011 the Canadian Industrial Security Directorate (CISD) has undertaken the revision of the risk management across its program responsibilities.

20. An off-site inspection prototype has been developed specific to the Canadian Industrial Security Directorate (CISD), in order to address the increasing number of new inspections. This approach is based on a measured risk management process and is used to conduct off site inspections on low risk files. This approach allows CISD to manage its resources efficiently by rendering

resources available to high risk file and provides an improved service delivery with a timely response.

21. CISD's diligent monitoring of security risks is being addressed by the continued promotion of the incident reporting requirements and, as an added precaution; this approach is further enhanced through the use of random unannounced inspections.

22. CISD proceeds with offsite inspections only if the risk is low. The factors considered for the determination of the risk are following criteria:

- Level of security required (For example, PROTECTED A information could be considered a low risk category depending on the assessment of the other factors listed below; while CONFIDENTIAL and SECRET or foreign classified information would fall into a higher risk category).

- Company compliance standing with the Compliance and Enforcement Policy (i.e. are they currently in good standing or are they under review)

- Company historical data on suspension and security breaches.

- Company recent data available to the public (Newspaper or TV info on irregularities)

23. Furthermore, internal integrity guidelines dictate that 10% of the approved off-site inspections will be validated via an unannounced on site physical inspection. The result of these inspections will guide CISD on the path forward with regards to its further refinement of this off-site prototype.

Risks/Disadvantages

- Limited information available on many companies in the program

- Cost of 'start up' – collection and storage of information

- Training for the individuals conducting the risk assessment

- Development of the criteria can become an 'industry' in itself

When it May be Appropriate To Use

- Where there is a need to focus any assurance efforts on those areas of greatest need, based on an understanding of the associated risks

- Where it is necessary to apply a defined assessment methodology that is transparent, documented and available for audit scrutiny?

- Where there is a growing gap between the volume of industrial security programs and available assurance resources.

Appendix 2

SOURCING OF INSPECTION/AUDITS – NETHERLANDS & FINLAND

Introduction

1. Industrial Security is fundamentally all about the 'sourcing' of activities required by Government that are to be provided by Industry. Therefore it might be argued that there is really little fundamental difference in the sourcing classified projects and the sourcing Industrial Security Inspections/Audits? The answer to this may depend on the level of assurance that is required and/or considered acceptable, i.e. the Risk Appetite. However, the more activities that are outsourced/sourced from Industry the less direct control is retained by Government – i.e. the Risk is increased.

2. The questions then become about how this increased risk is managed and the level of oversight that is required to be retained. The key question may be whether or not the consequences if things do go wrong are acceptable. Investigating and repairing the damage can be a costly exercise and the internal resource and expertise required to make reparation may have been lost when the activity was outsourced.

Methodology

3. During the period 2009 – 2010 the Netherlands DSA ran a short term pilot to 'outsource' Inspections and also ran a survey of MISWG participants to assess the extent to which 'outsourcing' was practiced and whether or not there were any legal impediments that would prevent its adoption. The findings of both the pilot and the survey were presented at MISWG 2010 and a 'lesson learned' paper developed by Netherlands and Finland was shared with MISWG participants in early 2011. In summary it was concluded that there was no real obstacle to Outsourcing/Private Hiring recognising that in some countries legislation does prohibit outsourcing. However, it is not a common practice in the Public Sector and whilst it would appear to be more common in Private Sector it is only in certain Industries and not generally for Security.

4. The 'lessons learned' paper raised further questions around the requirements for security clearances of outside Auditors/Inspectors and MISWG opinion was divided about whether or not it is possible to have an opinion on the level of protection of Classified Material without having access to it. Questions were also raised about what was considered to be true 'Outsourcing' and what would be considered Private or Public Sector 'Hiring'[10]

[10] See Definitions/Glossary of Terms – see Appendix 7

5. The Decision Tree at Annex to this Appendix has been developed to assist Authorities when considering the sourcing alternatives for security audits.

5.1 The following additional considerations should also be considered:

5.1.1 Supplier selection aspects

- Is the potential supplier qualified to undertake such activities?
- Is the potential supplier equipped to undertake such activities?
- Is the potential supplier really Independent/unbiased/impartial?
- Is the potential supplier a competitor or customer of the private Contractor?

5.1.2 Contractual aspects:

- Contract may require specific subcontracting provisions concerning sourcing partner (s)
- Will require Non-disclosure conditions; for example it is not allowed for the supplier to benefit from the work being done on auditing without prior written consent of the Authority. It is not allowed to disclose findings to third parties.
- Should make clear who has overall responsibility for managing the audits, e.g. who is signing the audit report.

5.2 Ultimately the Government Authority must retain oversight/control over the assurance/audit activities.

Benefits/Advantages

- The audit/inspection does not use own resources, so they may be utilised on other priorities
- Provides the ability to be specific about what is actually required .i.e. the assessor/auditor will do what they were tasked to do.
- Assessor/auditor can be more objective
- Report likely to be more detailed and written to meet requirement.

Risks/Disadvantages

- Auditor may need to be trained to required standard. e.g. to understand the context. This may lead to time and cost delays/increases.
- The Auditor may require access to Classified Material – is it possible to conduct Inspection/Audit without access to the material itself?
- Additional and/or hidden costs – auditor training and salary
- Issues about oversight/control.

- Potential for conflict of interest as the supplying Contractor gets insight information on security weaknesses (and potentially the commercial activities) of the recipient Contractor.

Where It May be Appropriate To Use

6. Recognising that outsourcing may not be an option that is considered appropriate in any circumstances, particularly where there is a legal impediment it is offered as a potential solution where there is:

- a need to involve extra audit capacity or expertise. E.g. when the workload for auditing Contractors exceeds the existing capacity within Industrial Security Authority.

- a significant degree of confidence/trust between the government Authority and the organisation being audited.

- a clearly defined and mutual understanding and agreement of the intent, conduct and required outcome.

Definitions

7. The following definitions refer to the Sourcing decision tree and complement the general definitions/glossary at Appendix 7.

- *Initial security audit*: a security audit at a private Contractor prior to the transfer of classified information to that private Contractor.

- *Private Auditor*: a private company or person qualified to conduct security audits at private Contractors.

- *Private Contractor*: the company subject to a security audit in the (future) need to handle classified information in the framework of a classified contract.

- *Private Hiring*: private person(s), working independently or for a private company or private person(s) will be hired temporarily to perform audits, as if they are part of the sponsors' organisation. The sponsor will be responsible for the execution of the audit. The activities necessary to process the gathered information into an audit report take place at the office of the sponsor.

- *Private Outsourcing*: a private company or private person(s) is contracted to perform audits. The private company or private person will be responsible for the execution of the audit. The activities necessary to

process the gathered information into an audit report may be conducted at the private company's or private person's office.

- *Public Auditor*: a public or governmental person or organisation qualified to conduct security audits at private Contractors.

- *Public Sourcing*: a public or governmental person or organisation is tasked to perform an audit.

- *Supplier:* the selected Private or Public Auditor to conduct security audits at private Contractors.

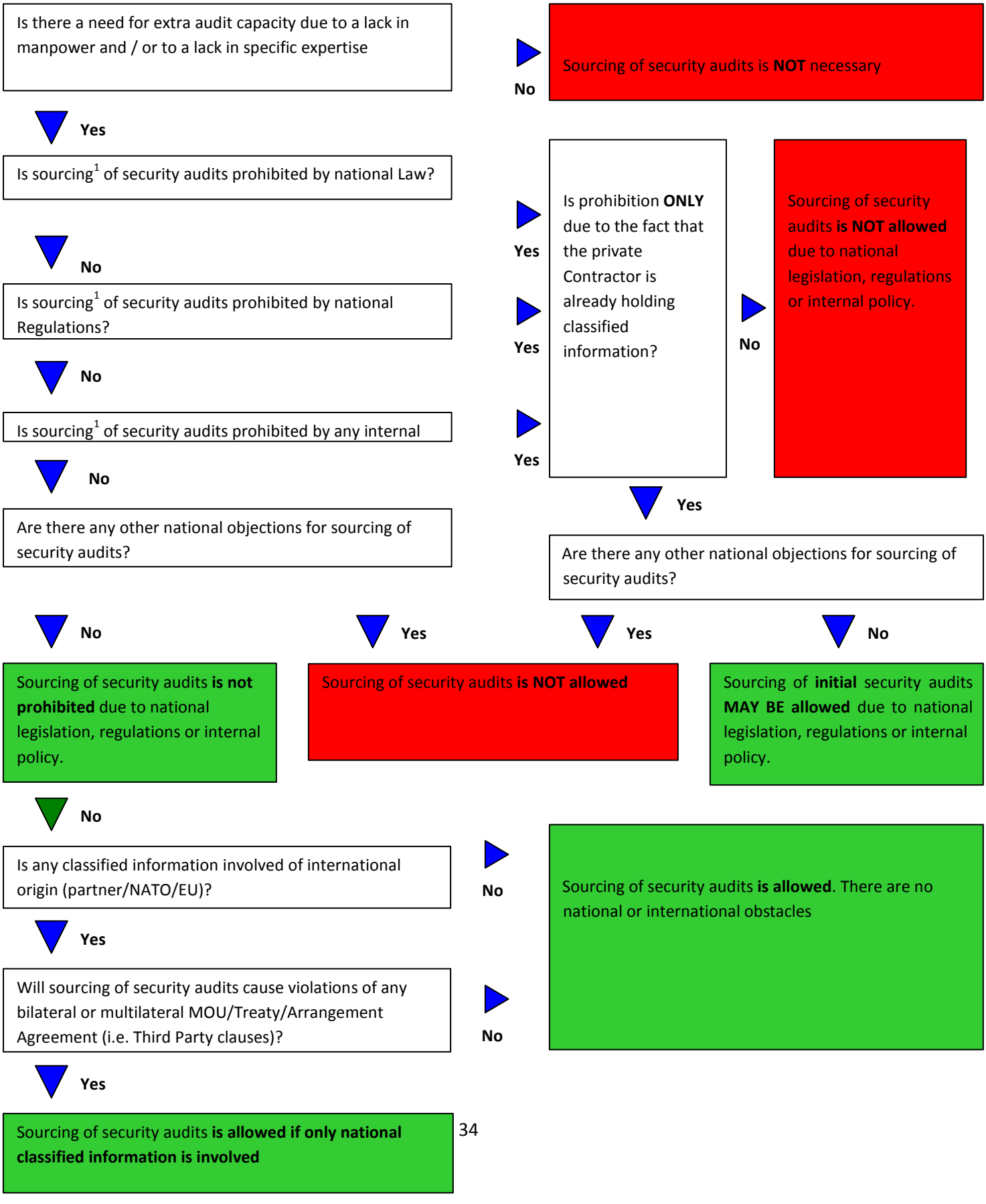
- *Recurring security audit*: a security audit at a private Contractor processing classified information (f.i. every 5 years).

- *Security Audit*: the process leading to a professional, unbiased, impartial and independent judgment on the quality of the security aspects of the object of the audit (i.e. private Contractor). The purpose is to provide assurance to the sponsor (i.e. government body), that classified information and material is/will be handled according to the security requirements.

(In this Appendix the term Sourcing is used for private outsourcing, private hiring and/or public sourcing.)

Annex to Appendix 2

Outsourcing Decision Tree



Appendix 3

CONTROLLED SELF ASSESSMENT – UK

Introduction

1. The UK MOD risk based strategy for continued Security Assurance in industrial entities granted a Facility Security Clearance (FSC) is based around a Controlled Self-Assessment methodology. The principle of operating a robust internal audit/inspection regime to assess risk management processes and to provide a corporate understanding of the level of risk being managed is a well understood quality management and audit methodology. The additional effect of such a regime is that, in most cases, it will assist the organisation to ensure risk reduction, and demonstrate that effect to an external assurance Authority.

2. At a time when resources are reducing, it is important that valuable effort from government Security subject matter experts should not only be directed at those facilities handling the most sensitive assets but also towards those where the most significant improvements are necessary i.e. the areas of greatest risk.

3. It is also important to recognise that organisations with a mature security capability are able to make the most effective and efficient use of their own resources where they can assert that the risks are understood and properly managed, in accordance with the requirements of national security.

4. It therefore seems sensible to conclude that it is in the mutual best interests of those within the government Security Assurance teams to work more closely with these potentially more experienced and qualified corporate security teams.

Methodology

5. The UK MOD strategy for implementing Controlled Self- Assessment as part of a more risk based approach to industrial Security Assurance oversight is as follows:

- At the instigation and with the approval of the Authority, where a company has multiple FSC cleared sites ***and*** a trusted Corporate Security team currently delivering an internal audit programme ***and*** an appetite to provide the UK MOD Security Assurance team (the Authority) with specified additional outputs; they will be asked to complete an annual self-assessment questionnaire.

- In accordance mutually agreed arrangements, the company will lead on the identification, assessment and prioritization of risks at their facilities. This may be undertaken as part of their existing internal audit arrangements.

- The company is required to afford the Authority, access to all internal audit reports and if required, to host an annual Assurance day where they will present this evidence in support of their self-assessment.

- This is then followed up with a coordinated application of the Authorities resources to minimize, monitor and control the risk eventuality based on the company's own assessment.

- The outputs from both of these activities are fed in to the Assurance Team's annual report, and will become the foundation for an objective risk based assessment of the appropriate extent of verification in the following year.

- Where concerns cannot be resolved the Authority reserves the right to initiate further action, as appropriate including where necessary on site Security Assurance inspections.

- In addition[11] the Authority will grant the Company the approval of extensions, changes of use, relocations of their business, subject to submission of a satisfactory data capture sheet and a minimum baseline measures matrix and the agreed maturity of their security capability. Novel or contentious changes will be managed through an agreed exceptional approval process.

- Any agreements/documentation relating to this process contain explicit references to remind the organisation/company that the UK MOD, as the Authority, continues to reserve the right to inspect or review any Company facility or activity operating at CONFIDENTIAL or above.

- The final decision to accept an organisation onto the programme rests with the Authority. Should organisational structure change, or for any other mutually acceptable reason, it may withdraw from the programme and revert to the Authority's standard review methods. The Authority may remove an organisation from the programme, with due notification and review of the reasons for such a decision.

6. Whilst acknowledging that a self-assessment approach is a recognised and accepted audit tool, it not a universal solution. Its application requires careful consideration and a robust, structured review and follow up process. In the UK MOD Controlled Self-Assessment is still under trial and is one a number of tools used by the Authority as part of its overall Security Assurance activities.

---

[11] The Authority will continue to inspect and approve 100% all new FSC applications including new sites, buildings or rooms, or significant changes to existing sites, or where a contract requires an increase in the protective marking of material to be held.

Benefits/Advantages

- Provides baseline 'compliance' evidence that could be analysed by government Security Assurance organisations.
- Reduces the size of the 'routine' inspection requirement and workload.
- Releases resources to support and audit more vulnerable Small/Medium Enterprises (SME's) or other at risk targets.
- Enable government inspection resources to be targeted against identified 'vulnerabilities', areas of highest risk or need (e.g. cyber threat)
- Delivers improved levels of commonality within multi-national or trans-national companies
- Risks identified where they maybe best understood and managed.

Risks/Disadvantages

- Not appropriate for SMEs who may have limited in-house security expertise.
- Reliant on the maturity and experience of company security structure/experts.
- Potential for company to try to 'hide' shortcomings.
- Reliant on the rigour and reliability of company audit function.
- May be perceived as a relaxation of government Authorities control/oversight.
- Removes an element of security 'intuition' and makes it more difficult to pick issues 'in passing'.

When It May be Appropriate To Use:

7. With large companies that are well practiced in risk management methodologies and generally welcome a risk-based approach to the provision of security assurance where there is:

- a significant degree of confidence/trust between the government Authority and the Company Security organisation.

- a mature/experienced security team and established security self audit and/or company internal audit arrangements in place.

- a clearly defined and mutual understanding and agreement of the intent, conduct and required outcome.

Appendix 4

INDUSTRIAL SECURITY REPORT – GERMANY

Introduction

1. The industrial security report is one way to adjust oversight in the field of industrial security to the level of risk of a facility. The report, which is in its introductory phase, will make it possible to inspect very low risk facilities remotely. This will allow to direct physical inspections to higher risk facilities, meaning a better allocation of resources.

2. All facilities granted a facility security clearance have traditionally been inspected physically by industrial security inspectors of the Federal Ministry of Economics and Technology. But not all facilities require the same level of oversight. For this reason, and in order to improve the allocation of resources, the Federal Ministry of Economics and Technology is introducing the industrial security report as an alternative to physical inspections.

Methodology

2. The industrial security report will replace follow-up inspections of very low risk facilities. These facilities will still initially be inspected physically, but follow-up inspections will take place remotely. The reporting process will comprise the following three steps:

- Firstly, the facility will receive information material and a questionnaire, and this will provide the basis for the facility's industrial security report. The information is designed to raise awareness of industrial security, give a repeated overview of industrial security and address typical errors and current questions.

- On the basis of this information, the security officer reports on industrial security in his facility by completing the questionnaire. The questionnaire covers important industrial security issues and typical errors. The facility security officer also has the possibility to ask questions.

- Finally, the report is checked by industrial security inspectors of the Federal Ministry of Economics and Technology and questions are answered. If the report gives no reason for concern, a physical inspection is dispensed with. However, the right to inspect the facility physically is reserved at all times.

3. It is the responsibility of experienced industrial security inspectors of the Federal Ministry of Economics and Technology to decide which facilities are inspected physically and which may submit a report. To qualify as a reporting facility, however, a facility must not store information classified CONFIDENTIAL or above, but rather send security-vetted personnel across to facilities granting

access to such information. Additional criteria are, for example, no or few and low value classified contracts and experienced facility security officers.

4. The industrial security report is in its introductory phase and will be adjusted according to practical experience and needs. The report is, however, already strengthening overall security by directing resources where they are needed most, away from very low risk facilities and towards higher risk facilities.

Benefits/Advantages

- Physical inspections are directed not to very low risk facilities, but to higher risk facilities, meaning a better allocation of resources.
- Resources are freed up, and time and effort of industrial security inspectors of the Federal Ministry of Economics and Technology can be focused on inspections of higher risk facilities.
- An appropriate level of oversight of and information about very low risk facilities is maintained.
- Travel costs, time and effort of industrial security inspectors of the Federal Ministry of Economics and Technology are saved.
- The facility security officer's awareness of industrial security is raised, because they have a more active part in the inspection process.
- The start-up costs for information material and the questionnaire are low, as are the operating costs.

Risks/Disadvantages

- The level of oversight on very low risk facilities may be perceived as being lowered, because it is adjusted to the potential risk of such facilities.
- The industrial security report requires the active collaboration of facility security officers, who must complete the questionnaire.
- The regular personal contact with the security officers of very low risk facilities, and the on-site impressions of industrial security inspectors of the Federal Ministry of Economics and Technology, are reduced.
- The industrial security report is not appropriate for higher risk facilities, which require a higher level of oversight and which therefore must be inspected physically.

Where It May be Appropriate To Use

5. Where a facility only poses a very low risk but under national laws and regulations there is a requirement to undertaken regular inspections. In Germany such a facility must for example:

- not store information classified CONFIDENTIAL or above, but rather send security-vetted personnel across to facilities granting access to such information and

- have no or only few and low value classified contracts and an experienced facility security officer.

6. Where a facility has an experienced security officer, who is willing and able to actively report on industrial security in their facility.

7. Where there is mutual confidence and trust between industrial security inspectors and facility security officers.

Appendix 5

PRIVATE COMPANIES & CONTRACTORS – SECURITY DIVISION – ISRAEL

Introduction

1. The Private Companies and Contractors Security Division at the Israeli Directorate of Security of the Defense Establishment (DSDE) directs close to 1000 small, privately owned companies and Contractors which serve the Israeli defense establishment. Due to the small size of these companies, a permanent security officer is not employed by them. However, due to their participation in classified defense programs, there is a clear need to provide them with security directives, and oversee their enforcement of these directives within the company.

2. These companies apply for and receive security clearance from DSDE, ranging in clearances from Unclassified to Top Secret. It also may be the case that the facility itself receives an Unclassified clearance, but the company employees receive PSC of Confidential or above. In these cases, the classified work is conducted outside the premises.

Methodology

3. Clearance is either requested by the company or initiated by DSDE, according to the relevant defense programs undertaken by the company. After the request is received, a risk assessment process begins at the Division.

4. This assessment ranks the company's risk factor and clearance accordingly, using the following criteria:

- Security classification of the program the company is involved in;
- Number of programs undertaken by the company;
- Number of employees;
- Dispersion of information throughout the facility;
- Sensitivity of information handled;
- Other factors (location, number of security mishaps in the past, overall impression of the security officer, etc.).

5. The company is ranked on a risk assessment scale which accumulates the score given on each criterion. The final score provides the Division with the information it requires in order to set the security classification for the company.

According to the score on the risk assessment scale, the Division decides what type of security officer will be assigned to the company, out of three options:

- Security Trustee: The trustee is an employee of the company itself, and is not considered a DSDE security officer. However, he is instructed and trained by DSDE according to the applicable security directives. The trustee must be able to direct and control all security issues within the company, and may, at times, be assisted by several other employees in various disciplines - physical security, information security, IT and communications, etc. Everyone company has a Security Trustee, regardless if they have an ASO or CSO as well;

- Audit Security Officer (ASO): The ASO is trained, guided and qualified by DSDE, and is not an employee of the company but paid and instructed by DSDE. He is charged with performing two-four inspections throughout the year;

- Cluster Security Officer (CSO): The CSO is trained, guided and qualified by DSDE, and is a retired employee of the Israeli security community. He is paid by the company, and works a minimum of 20 hours a week. He is formally and legally assigned to his position by DSDE for a limited amount of time, and is then placed under review and rehired according to his performance;

6. Inspections and audits: Approximately 250 inspections were recently conducted by all ASOs over the span of three months. The ASO receives an accurate assessment of the security status in the company according to various parameters, including but not limited to:

- Were program status reports submitted (yes/no);

- Have relevant processes been followed for the classification of items/programs (yes/no);

- Is a central registry kept for all classified informatio (yes/no), including written accounts;

- Are DSDE security directives present in the facility (yes/no);

- Are required logistical security devices found in the facility (paper shredder, etc.) (yes/no);

- Publications - Detailed account of all public company marketing;

- Presence and involvement of external entities - Cleaning service, Contractors, etc. and type and frequency of presence in the facility;

- Foreign presence and travel- Guests, foreign and domestic, including contacts of foreign visitors, seminars attended abroad by company employees, etc.;

- Does the company export its products/knowledge (yes/no), including presence of export and marketing licenses, list of countries exported to, records of shipments, etc.;

- Detailed account of the company's physical security infrastructure, to include locks, safes, sensitive areas, alarm systems, etc.;

- Detailed account of the company's computer and **IT** security means for use with classified information and data;

- Reliability - Detailed account of the employees and their security clearances

Benefits/Advantages

- Allows oversight and inspection of small industries and companies which are not directed by Authority according to law;

- Conservation of funds and resources, due to the fact that the companies pay their security officers;

- Allows Authority to focus on those companies with medium-high security clearance, or high risk;

- Provides Authority with direct contact with small companies;

- Companies have a designated point of contact for all security issues

- Allows for changes to be made to the security functions within the company on a relevant and continuous fashion

Risks/Disadvantages

- May not be appropriate/feasible where large numbers of smaller Defence Companies exist.

- May be difficult to implement where requirement for an FSC is not linked to granting of Personal Security Clearances (PSCs).

- Maybe difficult to implement FSC is not required for Classified Material that is RESTRICTED or below.

- Requires willingness of companies to fund security officers.
- Availability of appropriate resources e.g. Retired Officers to become CSOs.
- Requires separate arrangements to be made for CONFIDENTIAL and above.

Where It May be Appropriate To Use

7. Where the Authority has a requirement for oversight/inspection at Industrial facilities that are required to handle/store Classified Material below CONFIDENTIAL.

8. Where the Authority is confident the Industry are willing and able to co-operate in such a programme. E.g. there is a willingness/acceptance to fund the various inspection roles.

Appendix 6

INDUSTRIAL SECURITY CLEARANCES FOR {NATO}[12] CONTRACTS

Facility Security Clearances (FSC)

Issuing Facility Security Clearances

In accordance with {NATO} Security Policy requirements, the NSA/DSA of each {NATO} nation is responsible for granting a Facility Security Clearance for facilities located on their territory and which are involved in {NATO} classified contracts. Prior to issuing a FSC an assessment shall be made:

(a) of the integrity and probity of the company which is to be entrusted with {NATO} classified material at CONFIDENTIAL and above;

(b) of the personnel security status of owners, directors, principal officials, executive personnel, and employees of the facility, and of such other individuals who may, by virtue of their association, position or employment, be required to have access to {NATO} classified information or supervise a {NATO} classified contract, to ensure that they have the requisite level of PSC;

(c) of the foreign ownership, control and influence aspects (such as corporate structure) to ensure that these aspects are adequately addressed and where necessary mitigated; and

(d) of the security arrangements provided for the protection of {NATO} classified information to ensure that they comply with the requirements of {NATO} Security Policy and its supporting {directives}.

31. The following minimum criteria shall be applied by the NSA/DSA in issuing a FSC:

(a) that the company must establish a security system at the facility which covers all appropriate security requirements for the protection of NATO material and information classified at CONFIDENTIAL or above in accordance with NATO security regulations;

(b) that the personnel security status of personnel (both management and employees) who are required to have access to {NATO} classified material at CONFIDENTIAL or above is confirmed in accordance with {NATO} personnel security clearance requirements;

---

[12] References to NATO or NATO Classified (NC) have been included in {} to denote that these references maybe replaced with 'National' or other description, as appropriate.

(c) that the NSA/DSA has the means to ensure that the industrial security requirements are binding upon industry and that it has the right to inspect and approve the measures taken in industry for the protection of {NATO} classified information at CONFIDENTIAL and above; and

(d) that the company responsible for the facility shall appoint a Security Officer responsible for security who is in a position to report directly to an appointed member of the Managing Board of the company.

32. In granting a FSC, NSAs/DSAs shall ensure that they have the means to be advised of any circumstances that could have a bearing upon the viability of the clearance granted (e.g., a transfer of the controlling interests in the facility, a realignment of the business associations, the replacement of any of its principal officers or directors, or a change in the facility's physical location, an alteration to the premises it occupies, or a variation in its security procedures).

33. The NSAs/DSAs shall evaluate the extent to which the circumstances described above represent a threat to the security of {NATO} classified information that may be entrusted to that facility. If it is determined that there is a threat, the NSAs/DSAs will take appropriate steps to negate or mitigate the threat prior to issuing or maintaining the FSC.

34. The responsible NSA/DSA will verify the issuing of the FSC, when requested.

35. The NSA/DSA of a facility may specify additional security measures to be taken for the protection of {NATO} classified information in each such facility in its nation in order to qualify for a FSC.

Contractor Personnel Performing Works on NATO Premises, or on other Contractor's Facilities

36. Contractor, or sub-Contractor personnel including freelance consultants and interpreters, or any other type of freelance personnel or self-employed service providers, who carry out works on {NATO} premises, or Contractor's facilities in connection with a classified {NATO} project/programme or any other type of {NATO} classified contract requiring access to {NATO} classified information {NC}, or above shall hold a PSC at the requisite level.

37. The facility of the Contractor/sub-Contractor shall also hold a FSC without storage capabilities for {NC} and above where required by applicable national regulations.

38. {NATO} classified information made accessible to such personnel on {NATO} premises or Contractor's facilities shall be treated as if officially provided to the Contractor or sub-Contractor.

39. In case {NATO} information classified {NC} or above needs to be removed by a Contractor from {NATO} premises, or from Contractor's facilities, the Contractor's facility shall hold a FSC with storage capabilities for {NATO} classified information at the requisite level.

Changes to or Revocation of Facility Security Clearances

40. Should an NSA/DSA change or withdraw a FSC that it has issued, the NSA/DSA shall at once notify any other NSA/DSA or {NATO Programme/Project Management Agency/Office} to which it has provided a clearance notification.

41. If a FSC is revoked or withheld from a facility by its parent NSA/DSA, that fact must not be disclosed to the facility by another NSA/DSA, except with prior permission from the parent NSA/DSA.

Appendix 7

DEFINITIONS/GLOSSARY OF TERMS

- **Assurance**

Assurance forms part of corporate governance structure that provides accurate and current information about the efficiency and effectiveness of an organisations policies and operations, and the status of its compliance with the statutory obligations.

- **Audit Outsourcing**

A private company or person (s) is contracted to perform audits. The private company or private person will be responsible for the execution of the audit, after the proper accreditation process. Their activities necessary to process the gathered information into an audit report may be conducted at the private company or private person's office, properly certified if it contains classified information.

- **Classified Contract Sponsor**

The body with the authority to actually let classified contracts – the contractual authority.

- **Classified Information**

NATO Definition: Any information (namely, knowledge that can be communicated in any form) or material determined to require protection against unauthorised disclosure and which has been so designated by a security classification

Alternative Definition: Any information related to the national interest that may qualify for an exemption or exclusion under the Access to Information Act or Privacy Act and the compromise of which would reasonably be expected to cause injury to the national interest.

- **Compliance**

Compliance may be defined as the confirmation that the undertakings and or activities meet the requirements of accepted practices, legislation, prescribed rules and regulations, standards, terms of reference, an agreement, benchmark and or conditions of a contract.

Alternative definitions: Conformity, obedience, co-operation, observance and agreement.

- **Compliance Audit/Inspection**

Audit/inspection undertaken to confirm whether a company or organisation is following the terms of an agreement or the rules and regulations applicable to an activity or practice prescribed by an external agency or authority.

- **Compliance Assurance**

An evaluation method that uses a specified set of principles and standards to assess the quality of an organisation's reporting of its performance and its underlying systems, processes and competencies that underpins its performance. Inherent in this concept is an idea of oversight. The mechanisms by which oversight is exercised are negotiable, but in order to be able to give the assurance, oversight must have been exercised.

- **Compliance Process**

Measures instituted by an organisation to ensure that the provisions of its regulations are being met.

- **Contractor**

Private company required to manage/handle classified information, within the framework of a classified contract and subject to security assurance audits.

- **Facility Security Clearance (FSC)**

NATO Definition**:** An administrative determination by a NSA/DSA that, from a security viewpoint, a facility can afford adequate security protection to NATO classified information of a specified classification or below, and its personnel who require access to NATO classified information have been properly cleared and briefed on NATO security requirements necessary to perform on the NATO classified contracts

Alternative Definition: An administrative determination that an organization is eligible, from a security viewpoint, for access to CLASSIFIED and, if necessary PROTECTED, information or assets of the same or lower classification level as the clearance being granted.

- **Inspection/Audit Sponsor**

National Security Authority (NSA)/ Designated Security Authority (DSA) i.e. the body charged with overall responsibility for Assurance planning and oversight.

- **'On site' Inspection**

Face to face inspection to determine if the contractor (auditee) complies with physical, personal, ICT and/or other security requirements.

- **Private Hiring**

Private person (s), working independently or for a private company will be temporarily hired to perform audits, as if they are part of the sponsors' organisation. The sponsor will be responsible for the execution of the audit. The activities necessary to process the gathered information into an audit report take place at the office of the sponsor.

- **Risk**

NATO Definition: The likelihood of a vulnerability being successfully exploited by a threat, leading to a compromise of confidentiality, integrity and/or availability and damage being sustained.

Alternative Generic Definition: A risk can be defined as an event or circumstance causing a vulnerability to be exploited. This may bring about injury to employees, assets and threaten an organisation's ability to achieve its objectives.

- **Risk Appetite**

The level of risk that an organisation is willing to accept.

- **Risk Assessment**

The process of identifying security risks, i.e. the threats and vulnerabilities, determining their magnitude, and identifying areas needing safeguards or countermeasures.

- **Risk Context**

The context of risk management i.e. the risk context will affect the approach taken to address/mitigate risk.

Consideration should be given to the following:

- At which level of the organisation is risk management taking place?
  - strategic
  - programme
  - project
  - operational

- What kinds of risk are in prospect?
- What (broadly) will be the consequences of their occurring?
- Which stakeholders are important.

- **Risk Management**

A systematic approach to determining which security counter-measures are required to protect information and supporting services and resources, based upon an assessment of the threats and vulnerabilities. Risk management involves planning, organising, directing and controlling resources to ensure that the risk remains within acceptable bounds.

- **Security Audit/Inspection**

The process (post the initial FSC) leading to a professional, unbiased, impartial and independent judgement on the quality of the security aspects of the subject of the audit/inspection, to provide an assurance to the Authority that Classified Information and material is/will be handled in accordance with the relevant security requirements.

- **Security Authority**

National Security Authority (NSA) or Designated Security Authority (DSA).
i.e. the Government body with overall ownership responsibility (planning and oversight), FSC authority, and inspection sponsor.