Site Characterisation Survey

Introduction	
Date:	
Name of Facility:	
Address:	
Organisations(s) in residence:	
Business:	
Prepared By:	
Location Type:	
1st Review Date:	
2nd Review Date:	
3rd Review Date:	
4th Review Date:	

Site:

Overview

Prior to the arrival of the full Security Risk Assessment (SRA) team the Security Focal Point shall completed this Characterisation Survey for the SRA team for review and site familiarisation.

The form has been designed to:

- Identify the site assets, the severity of consequences of a security incident, or other harm to the assets.
- Provide the basis for the determination of the attractiveness of assets to potential adversaries.
- Identify the existing security precautions.
- Provide the basis for the identification of Principal Assets.
- Record locally assessed current threat levels

Additionally, the Security Focal Point will add any other relevant background, information or intelligence that is relevant to the Risk Assessment.

The Security Focal Point will provide the "Locally Assessed Threat Levels" for Robbery, Burglary, Theft – employee, Theft, Violent Crime, Fraud, Theft of information, Activism, Wilful Damage and Other Local Threats that may exist.

Step 1 - Security Risk Assessment Team Register			
Position	**Name**	**Email**	**Phone**
Facilitator / Leader			
Security Focal Point			
Process Safety & Operations			
Security Advisor Lead			
Security Advisor			

Site:

Step 1 - Scope and Threat Assessment	
Scope:	A high level physical and operational security review of (site). The intention of such an assessment is to review the Security Risk to People, Assets, Environment and Reputation with the combined function of the Likelihood of Consequence and the Severity of Consequence from either an Adversarial or Non-Adversarial Security Threat.
Concerns:	
Threat Assessment:	

Office Site Security Management		
1.	Is there clear delegation of security responsibility to a Security Supervisor/Manager or Focal Point? **Comment:**	Y/N

2.	If you answered yes to Question 1:	
	Does a formal job description exist for the security function?	Choose an item.
	Is the individual trained for the security function?	Choose an item.
	Does the supervisor lead a security department?	Choose an item.

3.	Are funds routinely budgeted for manpower and the purchase, maintenance and upgrade of security equipment / systems? **Comment:**	Y/N

Security ARSCI Chart	
4. Please complete the following ARSCI organogram depicting Security Accountabilities, Responsibilities, Supporting, Consulted and Informed roles.	
Who is RESPONSIBLE for security onsite?	
Who is ACCOUNTABLE for security onsite?	
Who is SUPPORTIVE for security onsite?	
Who is CONSULTED with regard to security onsite?	
Who is INFORMED about security matters onsite?	

DEFINITION OF PARTIES

Accountable*
Accountable, approves, must “sign off” acceptance of results.
The Accountable Party approves the work done by the responsible party and is accountable for the results.

Responsible*
Responsible to do it or get it done: The executing party. The responsible party executes the necessary work and takes the actions required to ensure compliance with legal and Company requirements.

Supportive
Provides support to the Responsible Party and to the Accountable Party.

Consulted
Will be consulted by the Responsible Party on activities and results. Will be given the opportunity to contribute.

Informed
Will be informed of decisions, activities and results, but not necessarily consulted.

(*= Mandatory positions)

ACTIVITY	PARTY (Please provide names)

Site:

	Country CEO	Head of Business	Location Manager	Asset Manager	Security Focal Point	Security Consultants	Other (Specify)		
Names									
Threat Assessment									
Operating Level									
Security Management System									
Security Documentation									
Security Self-Assurance Reviews									
Staff Security Awareness Training									
Contractor Security Awareness Training									
Liaison with Authorities (Police, Customs, etc)									
Liaison with Industry Contacts									
Other (Specify)									

Security Policy

5.	Does the company have a well-publicised security policy to promote awareness of the security approach? **Comment:**	Y/N

6.	If you answered yes to the question above:	
	Does the policy state clearly that the security approach is a joint effort of the authorities, the site operator and any contractors?	Choose an item.
	Is the policy and approach communicated to the government contractors and/or other parties?	Choose an item.
	Is the policy and approach reviewed periodically? **Comment:**	Choose an item.

Awareness		
7.	Is there a formal staff security awareness programme? **Comment:**	Y/N

8.	Is the level of security awareness and understanding periodically tested?	Y/N

Security Risk Assessments and Self-assessments		
9.	Are fully documented Security Risk Assessments undertaken every five years? **Comment:**	Y/N

10.	Are fully documented Security risk Assessments updated annually in the intervening period based upon changes in threat or materiality? N/A	Y/N

11.	Are self-assessments on security issues held periodically?	Y/N

12.	If you answered yes to either of the above:	
	Are recommendations acted upon?	Choose an item.
	Is there a follow-up check on the implementation of recommendations?	Choose an item.

13.	Please add any relevant comments (Please attach the most recent reports) – have obtained all relevant info

Site:

Security Plan	
14. Is there a site-specific Security Plan? (Please provide the most recent Security Plan) **Comment:**	Y/N

15. Who holds detailed plans relevant to the security of the site? Please provide to the team.	

Security Operating Levels	
16. Does the site utilise a Security Operating Level procedure?	Y/N

17. What is the current Operating Level: Green (Baseline), Amber, Red or Black?	Choose

Shared Offices	
18. Is the building or site shared with any third parties?	Y/N

19. If yes, please provide some detail as to who the parties are and reason for being on site.

Access Controls
20. Please outline the Access Control System for employees, contractors, vendors and visitors :
Employees – Contractors – Visitors –

Property Inspection and Property Search Programmes
21. Please outline the Property Inspection and Property Search Programmes.

Personal Searches

22.	Please outline the procedures for Personal Searches.

Property Removal Controls	
23.	Please outline the procedures for Property Removal Controls.

Mailroom Activities	
24.	Please outline the Mailroom Activities procedures.

Key Control Programme	
25.	Please outline the Key Control Programme.

External Doors		
26.	Are external doors secured?	Y/N
27.	Are doors of solid wood construction?	Y/N
28.	Are doors fitted with industrial grade (high-security) deadbolt locks?	Y/N
29.	Please outline any other relevant information regarding external doors.	

Windows and Roof Vents		
30.	Are windows and roof vents secured in accordance with Risk Assessments?	Y/N
31.	Please outline any relevant information regarding windows and roof vents.	

Site Perimeter		
32.	Are all facilities located within Company grounds?	Y/N
33.	Please provide an outline description of the site perimeter.	

Car Parking	
34. Are there designated car parking areas for staff and others?	Y/N

35. Please outline car parking facilities.

CCTV	
36. Does CCTV cover the Office or site?	Choose an item.

37. Please provide an outline of the CCTV System(s)?

Intruder Alarm	
38. Does Intruder Alarm System(s) protect the Office or site?	Y/N

39. Please provide an outline of the Intruder Alarm System(s).

Exterior Lighting	
40. Is exterior lighting installed? UPS	Y/N

41. Please provide an overview of the exterior lighting installation.

Emergency Lighting	
42. Is emergency lighting installed?	Y/N

43. Please provide an overview of the emergency lighting installation.

Lighting Installation Maintenance	
44. Is there a lighting installation maintenance plan?	Y/N

Site:

Guarding		
45.	Is the office / site guarded?	Y/N
46.	If so, which type of guard service is used (e.g. Contract Guards or Company staff)? Type of Service :	
47.	Have standards been developed for guarding services (e.g. reliability, punctuality, integrity, appearance, vigilance, customer focus, flexibility, competence, communication skills)?	Y/N
48.	Are guards properly trained (in e.g. observation, access control, patrolling, searching, incident response, HSSE, First Aid, use of equipment)?	Y/N
49.	Do guards have on display a Certificate of Approval and is their employer a licenced security guard company?	Y/N
50.	Are written, clear and unambiguous instructions given to all guards?	Y/N
51.	Are guards checked for understanding of the instructions?	Y/N
52.	Are guards adequately supervised (supervisor visits, patrol clocks, communication with control room)?	Y/N
53.	Do guards have proper resources (e.g. uniform, protective clothing, torch, whistle, baton, radio/telephone/mobile phone, transportation)?	Y/N
54.	Are guards backed up by a response team in case of a serious security incident?	Y/N
55.	Are professionalism and reaction times by the response teams checked regularly?	Y/N
56.	Has a maximum response time been formally agreed?	Y/N
57.	Are guards given adequate rest periods and facilities (e.g. shelter, food, toilets)	Y/N
58.	Are duties carried out on an 8- or 12-hour shift basis?	
59.	Please add any relevant comments?	

Incident Reporting		
60.	Does the site have an internal incident reporting system consistent with HSE requirements?	Y/N

61.	Are security incidents reported, recorded and investigated?	Y/N
62.	Have there been any major security incidents in the past?	Y/N
63.	Is there currently violence in/around the site/area of operations	Y/N
64.	If so, were remedial actions taken?	Choose an item.
65.	Can you please provide some detail as to any remedial actions taken:	
	Comment:	

Pre-Employment Screening		
66.	Is there a pre-employment screening procedure for employees and contractors?	Y/N
67.	Is there a procedure to screen and monitor all major suppliers, contractors, sub-suppliers, joint-venture partners and other major business associates on human rights/social issues?	Y/N

Information Security		
68.	Does the Office adhere to a Standard for the protection of information?	Y/N
69.	Please outline procedures covering locking away of documents at end of working day, securing of PC's, confidential waste disposal, clear desk policy, "out of hours" checks:	

Cash and High Value Items		
70.	Please outline any cash or high value items stored:	

Security Contingency Plans		
71.	Are there contingency plans in place?	Y/N
72.	Do these plans cover all assessed relevant credible threats (e.g. business continuity, bomb threats, fire and/or explosion, death or serious injury, site / installation evacuation)?	Y/N

73.	Are plans adequate, fit for purpose, up to date and reviewed regularly?	Y/N
74.	Are plans coordinated with local law enforcement, fire protection, private security contractors, other emergency response agencies, contractor companies and any neighbouring companies?	Y/N
75.	Are practical exercises held regularly?	Y/N
76.	Please add any relevant comments.	

Emergency / Crisis Response Organisation		
77.	Is there an emergency/crisis response team?	Y/N
78.	Does this team have full authority to make crisis management decisions?	Y/N
79.	Does this team operate from a predesignated and properly equipped crisis management room?	Y/N
80.	Is liaison with authorities included?	Y/N
81.	Are exercises held regularly (desktop, procedures, roles and responsibilities, etc?)	Y/N
82.	Please add any relevant comments.	

Liaison		
83.	Are relevant third parties (e.g. police, fire brigade) informed about the specific features of the site?	Y/N
84.	Are relevant third parties aware of the threat assessment made for the Office and the consequent security measures and response procedures?	Y/N
85.	Are meetings held regularly with relevant third parties to discuss security arrangements and issues?	Y/N
86.	Do relevant third parties share information on the latest security threats (early warning and indicators)?	Y/N
87.	Are relevant third parties involved in exercises?	Y/N
88.	Do any third parties have a formal role in the emergency/crisis response team?	Y/N
89.	Please add any relevant comments?	

Other Aspects
90. Please outline any other office security aspects that have not otherwise been addressed in this questionnaire.

Photographs
91. Please attach any photographs that you believe may be useful.

Principal Assets
Based upon the data provided in this Form, please list the Principal Assets of the site / office:

Locally Assessed Current Threats	
Please rate the likelihood for the below threats	
THREAT	**THREAT LEVEL** **Unlikely / Low / Medium / High / Extreme**
Robbery	
Burglary	
Theft - employee	
Theft	
Violent Crime	
Fraud	
Theft of information	
Activism	
Wilful Damage	
Other (please specify)	