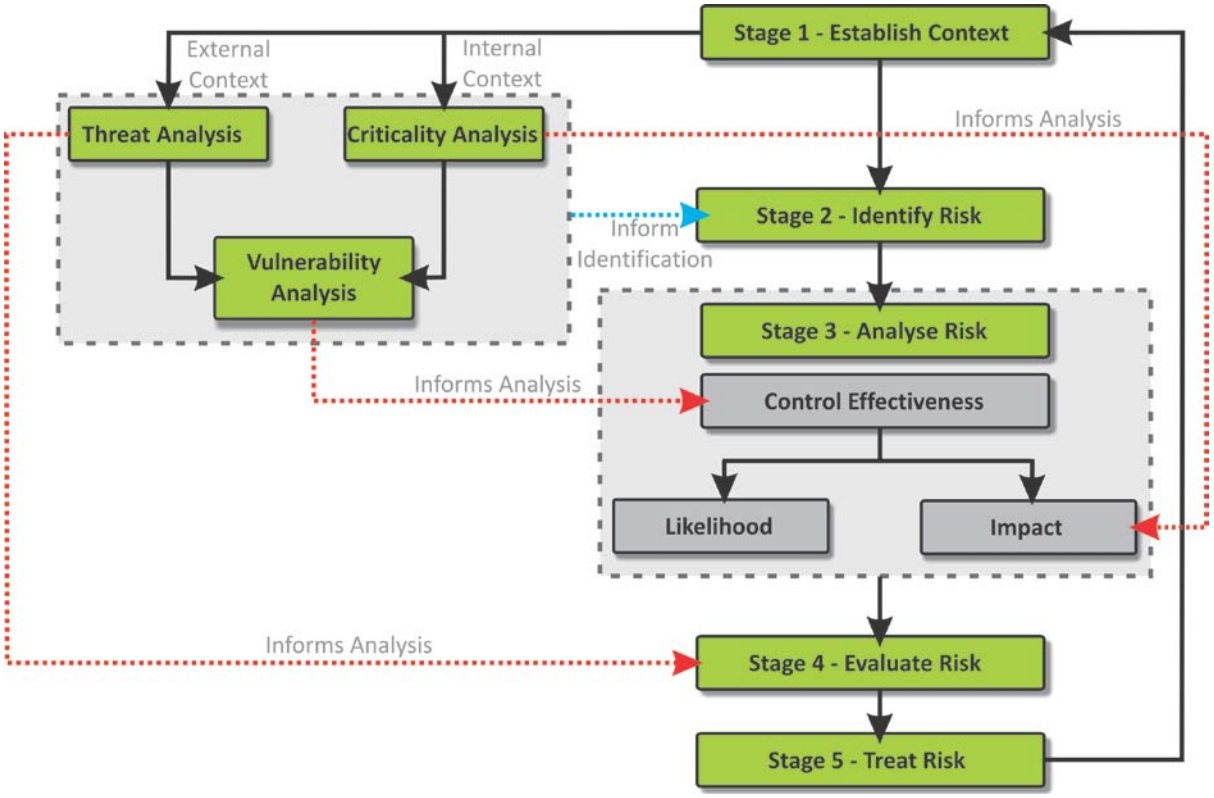
XTRAVISION (Pty) Ltd SECURITY RISK ASSESSMENT METHODOLOGY

Part 1

XTRAVISION follows the internationally recognized Risk Assessment Methodology that is compliant with ISO 31,000 Risk Management Standard and AS/NZ 4360 and the associated Hand Book 167 – Security Risk Management Standard as shown below.



Risk Assessment Flow Diagram

1. Cost Effective Solutions

XTRAVISION's Risk Assessment (SRA) methodology enables organizations, and individuals, to realize opportunities by focusing on what they want to achieve and how they intend to achieve it. XTRAVISIONELITE helps clients identify and understand the critical elements of their business, operation or project, relative to the security threat environment, enabling specific recommendations to be made to ensure cost effective mitigation of risk when and where it is needed.

2. Improved Confidence and Capability

XTRAVISION risk assessments add real value to the business by identifying the cost benefits of security measures and by enhancing strategic decision making capability. In addition, it creates a legacy system that potentially saves costs by transferring to the client the ability to continuously monitor security risks thereby allowing selection of cost effective and fit for purpose security solutions under the direct ownership and management of the client. This approach improves resilience, security and cost management as well as stakeholder confidence in the resilience of the organization through demonstration of a robust risk management process.

3. Definitions

It is important first to define what exactly is it that we are analysing when assessing an organization's security risks. XTRAVISION has developed the following definitions with consideration to international

risk management standards and the broadened definition of security considered in the human security paradigm.

Security Threat is anything originating from both a human, non-human and natural source that might affect the business objectives and the security of the people and assets which constitute an organization or business.

Security Risk is the Likelihood and Impact of an event, derived from a Security Threat, the consequence of which cannot be fully controlled by the entity in question, and for which an extraordinary response may be required to protect the achievement of business objectives.

4. Risk Assessment Stages

4.1. Stage 1 - Establish the Context

XTRAVISION's Consultants will work closely with our clients to achieve a sound knowledge of the client's business, its activities and future ambitions as well as the constraints under which it must operate. It will discuss previous Loss Data or incidents that have historically affected the organization's operations and will identify those assets critical to the achievement of the business objectives. Our Consultants will work with our clients to confirm the most appropriate Risk Framework that they can use to manage risk with due consideration to the client's Risk Tolerance, Risk Consequence and Risk Response. Wherever possible we will use the client's risk management criteria but in the absence of these we will adopt the most appropriate set of risk criteria based on international best practice.

4.2 Stage 2 – Identify Risk

XTRAVISION's Risk Consultants, in consultation with the client, will assess the security environment and associated risks and consider how those risks might affect the most critical assets of the project or organization under review. This will be achieved through individual and workshop discussions as most appropriate. Three tools assist in the identification of security risk:

The **Threat Assessment** identifies threats to the security of the organization's assets using advanced data mining software and bespoke search parameters. Security threat will consider: Regional, Criminal, Inter-State, Extremist, Economic, Environmental, Health, Accidental, Operational and Natural threats to the security of the subject of interest. Threats will be prioritized in terms of assessed Intent/Potential and Capability e.g. the Intent of a Criminal actor, or the potential of an Earthquake to disrupt business objectives.

The **Critical Asset Assessment** identifies what is most important to a business, organization, or project, to maintain key processes and to ensure business objectives can be achieved. Assets are defined as; people, physical, information and IT and Communication Technology (ICT).

The **Vulnerability Assessment** is consists of two elements; Pre Incident Vulnerability, focusing on Target Attractiveness and the ease of access to critical assets and Post Incident Vulnerability which focuses on Emergency Response Plans (ERP) of the organization and external agencies, Crisis Management (CM) capability, Business Continuity Planning (BCP) and Business Recovery capability (BR), in line with international standards such as BS25999.

4.3 Stage 3 & 4 – Analyse & Evaluate Risk

Identified security risks are now assessed by the risk assessment team in terms of the likelihood of identified risks materializing and what impact they might have on the critical assets identified if they do. In close consultation with the client, the risks to critical assets will be evaluated and a treatment priority established to determine which risks must be considered as a matter of urgency and which may be mitigated as part of the day to day business activity.

4.4 Stage 5 – Treat Risk

Occasionally an organization may wish to exploit a risk to achieve a specific business objective, however, it is more likely they will decide to accept, share or mitigate the risk through insurance, mutual aid programs or by limiting the likelihood or consequence should the risk occur. With the decision made on how the various risks are to be treated the security risk assessment is effectively completed with the SRA acting as the input for the development of the Security Mitigation Plan.

5. Development of the Security Mitigation Plan

XTRAVISION is able to draw on its extensive network of specialists to help the client develop the most appropriate and cost effective mitigation plan to manage the security risks identified in the SRA. The mitigation plan will initially focus on the development of a Strategic Security Plan (sometimes referred to as a concept of operations) presenting options as strategic functional or operational requirements for the Procedural, Manpower, Physical and Technology aspects of a security mitigation strategy.
XTRAVISION will always seek the client's agreement to the strategic security plan before moving on to develop the operational or functional requirements in greater and sufficient depth to facilitate the development of detailed design drawings in order to ensure to enable the final solution matches the client's needs, budget and project timeframe.

XTRAVISION SRA ASSESSMENT CRITERIA

Definitions:

- **Security Threat** is anything originating from both a human and natural source that might affect the security experienced by individuals and groups making up an organization".
- **Threat Source** is the point at which a Security Threat originates be that a natural or human source.
- **Threat Driver** is the motivation of a human source or the trigger event for a natural threat to occur.
- **Security Risk** is an event which originates from a Security Threat and whose consequence cannot be fully controlled by an affected party, and for which an extra ordinary response may be required to protect people, information or assets critical to the achievement of objectives or the processes that support them."
- **Risk:** Defined as *"The **effect** of **disruption** on **objectives**".*
- **Risk Source**: *"Those potential sources that could cause harm to an organisation".* The Risk sources may be external or internal and those considered include risks resulting from:
  - Crime;
  - Operations;
  - Accidents;
  - Health Hazards / Risks to Public Health;
  - ICT Related Risks;
  - Extremism;
  - Military Conflict;
  - Environmental;
  - Natural Hazards and Disasters

1.1 Threat Source Assessment Matrix

In assessing the threat, both the capability and intent of the threat source (or capacity to do harm and potential to do harm in the case of natural threats) are considered and awarded values in accordance with the table shown below.

Threat Level Summary		Intent (Human) or Potential (Non- Human)				
		Low	**Little**	**Significant**	**Strong**	**Extreme**
Capability (Human) Or Capacity (Non-Human)	**Extreme**	Medium	Significant	High	Extreme	Extreme
	High	Low	Medium	Significant	High	Extreme
	Significant	Low	Medium	Significant	High	High
	Medium	Low	Low	Medium	Significant	High
	Low	Low	Low	Low	Medium	Significant

Threat Level Assessment Table

1.2 Intent and Capability Descriptors

Intent is represented by the covert, implicit or expressed aims, goals, objectives, desires, or directions of the threat source. Historical trend data, previous incidents, and intelligence can inform the assessment of Intent together with the motivational factors for such individuals, groups or threat sources.

Intent Level	Intent / Potential Descriptor
Extreme	• Potential Adversary / Threat Sources have a proven, determined and stated intent to act against asset type; • Adversary has implemented this threat against similar assets in the region in the last 2 Years.
Strong	• Potential Adversary / Threat Sources have a stated, determined but unproven intent against asset type. • Adversary has not implemented this treat against similar assets in the last 2 years but has done so in the last 5 years.
Significant	• Potential Adversary / Threat Sources have a stated but unproven intent to act against asset type; • Adversary has not implemented this treat against similar assets in the last 5 years.
Little	• Potential Adversary / Threat Sources have no stated intent but there is historical evidence to suggest a possible threat from similar sources. • Adversary has not implemented this treat before.
Low	• Potential Adversary / Threat Sources have no stated intent but there is no historical evidence of threats from similar sources.

Capability (of a threat originating in a non-human or human source)

Capability considers the following attributes of the *'adversary/aggressor'*:

- Skills
- Knowledge
- Access to resources (e.g. weapons, specialist equipment), finances and other resources;
- Numbers of attackers/adversaries
- Access to support networks, time

Potential/Trigger (of a threat originating in a non-human source)

Potential is represented by the existence of factors that might trigger the source of the threat e.g. a fault line as a trigger for an earthquake. Historical trend data and previous incidents can inform the assessment of potential together with the factors that might trigger such an incident.

Capability Level	Capability / Capacity Descriptor
Extreme	• Potential Adversary / Threat Sources have a proven capability and the resources to implement the threat effectively against asset type; • Natural threat source has been active in the last 2 years and similar conditions still exist.
Strong	• Potential Adversary / Threat Sources have proven capability but limited resources to implement the threat effectively against the asset type; • Natural threat source has not been active in the last 2 years and conditions have not changed.
Significant	• Potential Adversary / Threat Sources have moderate capability and limited resources to implement the threat effectively against the asset type; • Natural threat source has not been active in the last 5 years but conditions have not changed.
Little	• Potential Adversary / Threat Sources have very limited capability and access to very limited resources to implement the threat effectively against asset type. • Natural threat source has not been active in the last 5 years and conditions have changed to reduce the potential for the threat to occur.
Low	• Potential Adversary / Threat Sources have almost no capability and no resources to act against the asset. • Natural threat source has not been active in this region.

1.3 Threat Levels Description

The descriptors proposed below reflect the criteria used in assessing the intent and capability of potential threat sources/adversaries.

Risk Level	Description of Overall Threat, and Intent and Capability of potential Adversaries
Extreme 5	• A specific Risk Exists against the asset or there is consistent evidence of the incident occurring regularly at the facility in the past and is expected to occur again the future.
Strong 4	• A known and detailed Risk exists against the asset type or there is some evidence that the incident has occurred in the past at the facility and is likely to occur again in the future.
Significant 3	• A defined Risk against the asset type exists but is not specific to the asset or there is some evidence that the incident has occurred regularly in the past at the facility and may occur again in the future.
Little 2	• It is likely that a Risk exists against the asset type or that there is limited evidence that the event has occurred in the past at the facility and may occur on an irregular basis in the future.
Low 1	• A Risk is unlikely to exist against the asset or similar asset types, or there is limited evidence of the incident occurring sand it is not expected to occur in the future. • There has been no history of attacks / other Risk sources against similar assets in the region.

Description of Threat Levels

2. Criticality Assessment

Definition of criticality: *"The importance or dependence that an organisation has on a person, function, process, item, infrastructure or specific facility."*

For the purpose of this assessment, assets are defined as: People, Physical, Information, ICT, & Operational Process (incl. utilities and emergency response). Clearly not everyone and everything is critical to the functioning of the Facility and achievement of its objectives. However, some people, information, physical assets, facilities or systems are by their nature critical to normal operations and their loss or disruption as a result Risk event occurring could result in business or organisational failure, loss of student and faculty confidence, or damage to reputation.

The question to be answered is what is the criticality of the asset, facility or system, function or services if it is lost or disrupted as a result of a successful Risk or attack occurring? Once criticality and vulnerability are known risk treatment measures are defined and priorities applied in protecting the facility and its operations.

2.1 Criticality Rating

Criticality is assessed as: **Extreme**, **High**, **Significant**, **Moderate** and **Low** with consideration to the impact of the loss of functionality of the asset or process. Loss of the assets is assessed in terms of; cessation of critical process, short term recovery capability, serious or prolonged reputation damage and a proposed rating system for the facility is shown in the table below.

Criticality	Impact on Facility	Impact on Individuals
Extreme 5	• Complete cessation of all functions; • No Short Term recovery capability; • Serious prolonged reputational Loss (extending for many months)	• Catastrophic safety incidents (multiple fatalities, serious casualties); • Long Term Financial loss (e.g. loss of employment)
Strong 4	• Complete cessation of one or more facility key functions; • No Short Term recovery capabilities; • Serious prolonged reputational loss (extending for weeks or months)	• Multiple serious safety incidents (A fatality or several serious casualties); • Mid to Long term major financial loss (e.g. prolonged stand down of employment over several months)
Significant 3	• Complete cessation of one or more facility key functions; • Limited Short Term recovery capability; • Reputational loss on specific operations (extending for weeks or months)	• Major Safety incidents (multiple injuries requiring medical attention); • Financial losses extending over several weeks (e.g. contracts put on hold).
Little 2	• Reduced effectiveness of one or more facility key functions; • Short term recovery capability is possible; • Reputation loss 9extending for days or weeks).	• Safety incidents requiring first aid treatment; • Long term major financial loss (e.g. loss of employment).
Low 1	• Little impact on functions; • Recovery is immediately possible; • Little measureable reputation loss	• Insignificant safety implications; • No appreciable financial loss

Criticality Table Description

3. Vulnerability Assessment

When assessing the vulnerability of an organisation it should be considered as a 'system of systems' and each component and sub system examined for vulnerability to the defined security risks addressing: the nature of its business operations, its people and assets (property), business systems and processes, information, location and accessibility of its operating sites, and existing security controls in place (degree of permissiveness) within the business, and society, to counter the identified security risks, and potential impact to reputation should the Risk event occur. The combination of these factors determines the organization's vulnerability to assessed security risk.

The following were considered when assessing the vulnerability of the Facility assets, facilities, processes and systems to identified risks:

- **Visibility***.* What is the profile, visibility or iconic status of the asset, facility or system as a potential target for the Risks identified? Does the location and visibility of the asset, facility or system make it vulnerable to attack or disruption by Risk sources?
- **Attractiveness.** What is the attractiveness of the asset, facility or system as a potential target for criminals, extremists, protesters or other Risk groups?
- **Accessibility***.* How accessible is the asset, facility or system to potential Risks?
- **Resilience***.* How robust is the asset, facility or system to withstand attacks from identified Risk sources, what is its design or engineered protection and redundancy, repair and service recovery time, are continuity and recovery plans in place to enable service or operations recovery within agreed timeframes.
- **Collateral Exposure***.* Does the location of the asset and surrounding facilities expose it to greater risk or make it more vulnerable to attack, damage, systems disruption or local interference e.g. a facility sited next to a major O&G installation, fuel or chemical storage area, pipeline, high tension lines etc?
- **Interdependency.** To what degree is the asset / facility / system dependent on external agencies, supplies or systems for its normal operation, survival and recovery in the event of an incident e.g. power supply, supply chain, emergency services etc?
- **Controls***.* What security controls and systems are in place (or are required) to deter, defend / delay, detect, respond and recover from attacks should they occur, and how effective are they?

The vulnerability of each asset to each risk is assessed and this combined with the criticality of the asset, use to determine the Asset Risk Profile. By consolidating the risk profiles an overall asset risk profile is calculated which identifies the exposure of the asset to the risk universe and allows a priority of mitigation to be identified and appropriate measures to be applied.

The following sections describe the criteria by which each of the above are assessed with a brief description of the process.

3.1 Visibility

The facility/asset's profile may attract operational or security risk and the profile impact security risks.

In addition, the location of an asset may positively or negatively influence its security risk e.g. an unlit storage yard full of vehicles and building materials located alongside and in plain view of a road is at greater risk of losses from opportunistic break-in and theft than one in a less conspicuous location.

A proposed scoring system for visibility rating is included in the table below:

Visibility Rating	
Very High 5	• Asset has a very high visibility or public profile and or iconic or celebrity status, it has attracted local and international media attention or is widely known and considered symbolic of the company and country; • Asset is in a public and very visible location and may be easily accessed or observed from surrounding buildings or terrain.
High 4	• Asset has a high profile and or is easily recognised and has attracted local media attention, it may be considered symbolic or representative of the company and country; • Asset is in a high profile location and may be accessed or observed from surrounding buildings or terrain or by passing traffic.
Medium 3	• Asset has a medium profile and it could be recognised or considered symbolic or representative of the company and country; • Asset is in a medium profile location and may be accessed with difficulty and observed from surrounding buildings or terrain or with difficulty by passing traffic.
Low 2	• Asset has a low profile and it is not likely to be recognised or considered symbolic or representative of the company and country; • Asset is in a low profile location and cannot be easily observed from surrounding buildings or terrain or by passing traffic.
Very Low / Insignificant 1	• Asset has a very low profile and it is unlikely to be considered important or representative of the company and country; • Asset is in a hidden location and cannot be easily accessed without difficulty or observed from surrounding buildings or terrain or by passing traffic.

Visibility Rating Criteria

3.3 Target Attractiveness

The attractiveness of an asset to attack by potential Risk sources contributes to its vulnerability. A proposed rating system for rating profile is included in the table below:

Attractiveness	
Very High 5	• Asset represents a very attractive target to opportunistic or planned attack as a result of its profile, image or iconic status, critical importance to the facility's operations, high net worth or asset value, or exclusivity; • The asset represents a highly attractive target for the threat source e.g. Criminal, extremists or protest groups or vandals.
High 4	• Asset represents an attractive target to opportunistic or planned attack as a result of its profile, importance to the facility's operations, high asset value or exclusivity; • The asset represents an attractive target for the threat source e.g. Criminal, extremists or protest groups or vandals.
Medium 3	• Asset represents a possible target for opportunistic attack as a result of its profile and moderate importance to the facility's operations and moderate asset value; • A possible target for the threat source.
Low 2	• Asset represents a less likely target for opportunistic attack as a result of its low profile and limited importance to the facility's operations and low asset value; • It is an unlikely target for the threat source.
Very Low / Insignificant 1	• Asset represents an unattractive target due to its insignificance minimal importance to the facility's operations and insignificant asset value; • It represents a rare target for the threat source.

Attractiveness Rating Criteria

3.4 Accessibility

The ability of employees, members of the public and potential Risk sources to gain physical or logical access to assets, facilities or systems directly affects their vulnerability. This is normally countered by the careful positioning of critical facilities and use of security mitigation systems applied in depth, the application of physical and logical security, monitoring or surveillance of the asset and use of alarms to alert security to unauthorized access or tampering.

A proposed rating system for accessibility is included in the table below:

Accessibility	
Very High 5	• There is free and unrestricted public access to the asset with no active or passive monitoring, security presence or area surveillance; • Movement patterns and activity schedules (timetables) are openly publicised; • There is excellent geographical access and open approaches to the asset.
High 4	• There is unrestricted public access to the asset, there is only limited monitoring, security presence and area surveillance, and where appropriate, this is restricted to entry points only; • There is good geographical access and a number of road and across country approaches to the asset.
Medium 3	• Public Access is restricted to designated areas but flows around buildings and facilities in the immediate vicinity of the asset. • Where appropriate public access to sensitive areas is prevented and access is controlled; • Some monitoring and public area surveillance adjacent to the asset is undertaken and a normal security presence is maintained; • There is reasonable geographical access to the asset, although approaches are restricted and channelled by terrain vegetation.
Low 2	• No public access to the asset; • Staff access and movement within or adjacent to the asset is controlled; • Visitors are by appointment and may be escorted; • Where appropriate, active and passive monitoring and surveillance of the site and key points is undertaken; • Where appropriate a small on site security presence is maintained or periodic patrols monitor the asset; • There is limited geographical access to the asset and approaches are restricted.
Very Low / Insignificant 1	• Public Access to the asset is excluded; • Visitors require clearance and escort by a staff member at all times; • Staff Access and movement within or adjacent to the asset is strictly controlled or is on a needs basis; • Where appropriate active and passive monitoring of all the entry and exit points , key points and work areas are undertaken; • Security Guards are present on site and conduct regular and random patrolling of the facility; • There is restricted geographical access to the asset and approaches are monitored.

Accessibility Risk Rating Criteria

3.5 Resilience

Resilience is the robustness and ability of the asset, facility or system to withstand attack and / or maintain service in the event of damage or disruption. Resilience is generated by the combination of effective positioning, physical protection, inbuilt systems monitoring, control and redundancy through effective design and engineering, the inclusion of automatic back-up / fail safe modes, networked alternatives and disaster recovery plans and processes.

A proposed rating system for Resilience is in the table below. Note that the scoring system is reversed, with the highest control effectiveness rating (Extreme) having the lowest score (1) which is consistent with it offering the lowest level of risk. Resilience ratings:

Resilience	
Very High 5	• Asset, Facility or System is fragile with limited or no protection, inherent resilience or redundancy; • No immediate back up or alternative exists;
High 4	• Asset, Facility or system is moderately robust with some protection, inherent resilience and redundancy; • An alternate system or service is not immediately available but can be implemented with significant disruption to critical services or processes within agreed time frames (specific to asset, services or processes).
Medium 3	• Asset, Facility or system is robust with protection and inherent resilience and redundancy is built in but is restricted to sustainment of critical services or processes, and or is of limited endurance; • An alternate system or service is available and can be implemented with moderate disruption to critical services or processes within agreed time frames (specific to asset, services or processes).
Low 2	• Asset, Facility or system is robust and protected with inherent resilience and redundancy built in; • Switching to standby capability or an alternate process is automatic and restores restricted or full services within an agreed time; • Restoration of full services is planned for and possible within an agreed time frame.
Very Low / Insignificant 1	• Asset, Facility or system is very robust and well protected with high levels of resilience and redundancy built in; • Switching to standby capability is automatic with no loss of services.

Resilience Criteria

3.6 Collateral Exposure

An asset, facility or system may also attract risk exposure from collateral damage as a result of surrounding or co-located assets, facilities or systems as a result of their profile, attractiveness or volatility rating e.g. a telecommunications node located inside or alongside a volatile chemical storage facility may be considered at higher risk than one located in a green field site.

The exposure represents a calculation of the exposure of the Facility to losses or disruption which could result from a successful security breach, or loss of use or functionality of assets as a result of an incident to an adjacent asset (not owned or operated by the Facility.

A proposed rating system for collateral exposure is included in the table below:

Collateral Exposure	
Very High 5	• Asset, Facility or System is co-located with, or close to a facility that is iconic or very attractive as a potential target for criminal or extremist attack; • Is at risk from blockade or disruption through public protests; • Is at serious risk from collateral damage as a result of major accidents or industrial hazards in surrounding properties
High 4	• Asset, Facility or System is co-located with, or close to a facility that is attractive as a potential target for criminal or extremist attack; • Is at risk from blockade or disruption through public protests; • Is at risk from collateral damage as a result of major accidents or industrial hazards in surrounding properties
Medium 3	• Asset, Facility or System is co-located with, or close to a facility that could attract criminal interest or disruptive activity; • Is at medium risk from collateral damage from accidents or industrial hazards in surrounding properties
Low 2	• Asset, Facility or System is not co-located with, or close to a facility which is likely to attract criminal or other interest; • Is at low risk from collateral damage from accidents or industrial hazards in surrounding properties
Very Low / Insignificant 1	• Asset, Facility or System is not co-located with, or close to a facility which is likely to attract criminal or other interest; • Is at very low risk from collateral damage from accidents or industrial hazards in surrounding properties

Collateral Exposure Criteria

3.7 Interdependency

The interdependency of the facility and its operations on people, processes, data / information, ICT and physical infrastructure, systems, utilities, and supplies (logistics and services) and 3rd parties or external organisations affects its vulnerability. The dependencies must be considered individually and collectively. At facility level the interdependencies are considerable and will require careful analysis.

A proposed rating system for Interdependency is included in the table below:

Interdependency Vulnerability	
Very High 5	• Operations of Asset, Facility or Systems are totally interdependent upon services, supply and support from external agencies; • Loss of external services results in serious disruption to operations or the functionality of the asset; • Recovery from loss of external services would be complex and take significant time and engineering efforts; • There is no back-up facility or alternative provider.
High 4	• Operations of Asset, Facility or Systems are interdependent upon services, supply and support from external agencies; • Loss of external services results in major disruption to operations or the functionality of the asset; • Recovery from loss of external services would be prolonged and requires majors engineering efforts; • There is back-up and fail safe systems in place and an alternative provider has been identified.
Medium 3	• Some Operations of Asset, Facility or Systems are interdependent upon services, supply and support from external agencies; • Loss of external services results in moderate disruption to operations or the functionality of the asset; • Full recovery from loss of external services would be a routine procedure.
Low 2	• Few Operations of Asset, Facility or Systems are dependent upon services, supply and support from external agencies; • The Asset, Facility or Systems is largely self-contained; • Loss of external services results in minimum disruption to operations or the functionality of the asset; • Full recovery from loss of external services is automatic and can be established with low impact on operations.
Very Low / Insignificant 1	• No Operations of Asset, Facility or Systems are dependent upon services, supply and support from external agencies; • Loss of external services results in minimum or no disruption to local operations or the functionality of the asset; • Full recovery from loss of external services is automatic and no impact on operations.

Interdependency Criteria

3.8 Control Level Effectiveness

Security controls are designed to protect the facility and its assets by providing mechanisms for deterring, detecting, delaying / defending, responding to and recovering from Risks should they occur. Such protection may be achieved by the application of physical, logical, systems and procedural security and monitoring to enable Risks to be detected as they develop and to enable timely and appropriate investigation and response. Incident response is usually conducted by security personnel from within the organisation and / or contractor guard force, and then escalated to civil authorities. Serious or major incidents may be escalated immediately.

A proposed rating system for Controls is in the table below. Note that the scoring system is reversed, with the highest control effectiveness rating (Extreme) having the lowest score (1) which is consistent with it offering the lowest level of risk. Control ratings:

Interdependency Vulnerability	
Very High 5	• Controls are minimal or non-existent or it is extremely likely that any existing controls will be easily breached or will fail; • There is recent evidence of widespread control failures; • No contingency plans are in place to handle major breaches or to maintain or recover key services and processes.
High 4	• Some Controls are in place but do not mitigate all risks to the asset; • There is a high probability of controls being breached or failing; • There is recent evidence of some controls being breached; • There are few contingency plans are in place to handle major breaches or to maintain or recover key services and processes.
Medium 3	• Controls are in place and the majority are effective, however there is a moderate probability of controls being breached; • There is recent evidence of minor breaches of control measures; • There are some contingency plans in place to manage recovery of key services and processes in the event of a breach.
Low 2	• Controls are in place, functioning and effective; • There is a low probability of controls being breached; • There is recent evidence of minor non-compliance with controls; • Contingency plans are in place to manage recovery of a few key services and processes in the event of a breach.
Very Low / Insignificant 1	• Controls are in place, effective, the majority are functioning; • There is a very low probability of controls being breached; • There is no evidence of controls being breached; • Contingency plans are in place to manage recovery of all key services and processes in the event of a breach.

Interdependency Criteria

4. Likelihood (assessed probability of occurrence)

Likelihood is defined as ".the chance, probability or frequency of an event occurring." The likelihood definitions are based on actual historical, security Risk incident data and analysis or inferred for various sources. The likelihood (i.e. the probability of a Risk happening) is strongly influenced by the vulnerability of the asset to identified risks and the control level effectiveness which may mitigate the occurrence of the risk.

As a general rule, societies with high standards of governance, policing and public safety, and low levels of corruption, usually have commensurately low rates of crime and violence; offering a Low probability of such Risks developing and / or occurring. The reverse applies in societies with poor standards of governance and high levels of corruption, which provide a permissive environment in which criminal activities and violence may occur, attracting a higher likelihood and Risk rating.

The likelihood of an incident occurring as a result of an identified risk is therefore determined by conducting an analysis of the Risk level (intent and capability for the Risk to develop) and the chance of it occurring to the organisation in the environment in which it operates (vulnerability).

A proposed Likelihood table with descriptors is below:

Interdependency Vulnerability		
Almost Certain 5	• Is expected to happen in most circumstances	• Has occurred on an annual basis in this facility or similar organizations in the past or circumstances are in line that will cause it to happen • ≥90% probability of the event occurring
Likely 4	• Will probably occur in most circumstances	• Has occurred in the last few years in this facility or similar organizations or has occurred recently in other similar organizations; • ≥50 - 89% probability of the event occurring.
Credible 3	• Might occur at some time	• Has occurred at least once in the history in this facility or similar organizations; • ≥20 - 49% chance of event occurring in the next few years.
Unlikely 2	• Could occur sometime	• Has never occurred in this facility but has occurred infrequently in another similar organization.
Remote 1	• May occur only in exceptional circumstances	• Is possible but has not occurred to date in any similar facility or organization.

Likelihood Criteria

5. Consequence (assessed impact to facility)

Consequence is defined as: "The outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain." There may be a range of possible outcomes associated with an event.

The consequences of any security event are assessed with reference to the potential damage to the facility should the Risk occur and may be defined in terms of effect on the achievement of the facility objectives, or possible impact on meeting defined business, financial, management, operational, safety, security and environmental requirements, in terms of the legal and regulatory framework or impact to reputation.
The consequence definitions reflect the culture, risk appetite and thresholds, governing policies and operating or regulatory framework of the facility and are scaled to match the size and complexity of the clients operations, the culture of the organisation, and value of investment (assets and infrastructure) involved.

What may be of major consequence to Oil and Gas facility (e.g. major mechanical system failure) may be regarded as of minor consequence (albeit still an issue for management concern) for a major Facility.

Consequence has been assessed for the impact on:

- The Client's Reputation as a safe and secure;
- The impact on key operations; and;
- Impact on the local environment and sustainability aims of the client.

In analysis the consequence against likelihood the approach adopted for security risks in this assessment reflects international best practice ISO 31 000 (and HB 167) and is to take the most probable worst case scenario.

Taking the ultimate worst case scenario of any major security or disaster event usually results in catastrophic impact and mass destruction. Focusing on the improbable, 'absolute worse-case' (e.g. a

major earthquake that lays waste to the business leads to unrealistic Risk and risk assessments and over-engineered, or unaffordable protective measures.

Proposed Consequences ratings for the business and descriptors are in the table below.

Consequence	
Very High 5	• Catastrophic impact preventing achievement of the facility's objectives; • Prolonged and adverse media coverage with serious and prolonged reputation impact; • Significant disruption to the facility's operations; • Severe and long term environmental damage; • Loss of very sensitive information which has significant impact on reputation and or revenue.
High 4	• Major impact delaying achievement of the facility's objectives; • Extensive and short to medium term adverse media coverage with major reputation impact; • Major disruption to the facility's operations; • Major short to medium term environmental damage; • Loss of very sensitive information which has a major impact on reputation and or revenue.
Medium 3	• Moderate impact affecting achievement of the facility's objectives; • Short term adverse media coverage; • Moderate disruption to the facility's operations; • Moderate short term environmental damage; • Loss of sensitive information which has a moderate impact on reputation and or revenue.
Low 2	• Minor impact on achievement of the facility's objectives; • Local, minor adverse media coverage; • Minor disruption to the facility's operations; • Minor short term environmental damage; • Loss of sensitive information which has a minor impact on reputation and or revenue.
Very Low / Insignificant 1	• Negligible impact affecting achievement of the facility's objectives; • Minimal adverse media coverage; • No disruption to the facility's operations; • No environmental damage; • Loss of information has no impact on reputation and or revenue.

Consequence Assessment Criteria

6. Risk Assessment

Using the likelihood and consequence of occurrence of the untreated risk, the collective assessment of risk levels can then be graphically shown on a Boston Square to facilitate management decisions of appropriate treatment. The Boston Square reflects the risk appetite of the client and as such the table below, based upon best practice for a conservative risk appetite, represents a proposed table for approval by the client.

6.1. Boston Square Probability vs Consequence

Probability (From Likelihood Table)	Consequence (From Consequence Table)				
	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Almost Certain 5	Significant	High	High	Extreme	Extreme
Often 4	Significant	Significant	High	High	Extreme
Likely 3	Medium	Significant	Significant	High	High
Possible 2	Low	Medium	Significant	Significant	High
Rare 1	Low	Low	Medium	Significant	Significant

Risk (Untreated) in Boston Square

The descriptors given below for the response and management of the various risk levels is in line with international best practice and reflects the normal treatment for risks within the categories shown.

Risk Score	Risk Level	Description
9 - 10	Extreme	Requires highest priority of risk mitigation strategy and constant monitoring by senior management
7 – 8	High	Requires priority risk mitigation strategy and constant monitoring by line management
5 - 6	Significant	Requires priority risk mitigation strategy where no controls currently exist and constant monitoring by operational staff.
4	Medium	Risk mitigation measures should be considered and implemented within 6 – 12 months.
2 - 3	Low	Acceptable risk no action required

Risk Management Descriptors

6.2. Risk Treatment

Finally, the management of serious risk is considered with reference to the cost benefit of risk treatment options and the final step before determining the specific mitigation measures is to determine the risk management measures to be applied each risk.

Selection of the preferred treatment option is a management decision and should not be made by the security professionals in isolation from the key Facility management team.

The risk treatment options that the client will be asked to allocate to the identified risks are in line with ISO 31 000 and are:

- Avoid the risk by deciding not to start or continue the activity that gives rise to the risk
- Taking or increasing the risk in order to pursue an opportunity
- Removing the risk source
- Changing the likelihood
- Changing the consequence
- Sharing the risk with another party or parties (including contracts and risk financing)
- Retaining the risk by informed decision