

SECURITY RISK ASSESSMENT
for the
IDENTIFIED RURAL REGION
(A Rural Commercial Farming
Community)

A user-friendly template to facilitate a
Risk Assessment and Security Plan

AGRICULTURAL
OPERATIONS
ABC FARMING COMPANY



Unicornlpconsultant@gmail.com / 27739544450

TABLE OF CONTENTS

PARA	SUBJECT	PAGE
1	Introduction	3
1.1	Interviews	3
1.2	The Farm Visit	3
1.3	Background	4
1.4	Infrastructure	4
1.5	Mission	5
1.6	Analysis of the Mission	5
1.7	Restrictions on the Execution	5
1.8	Integrated Security Measures	6
1.9	Identification of Tasks	6
2	Vulnerabilities	6
2.1	Personnel	6
2.2	It Equipment and Information	6
2.3	High value controlled and vulnerable items	7
2.4	Other Aspects	7
3	Threats	7
3.1	Employees	7
3.2	Criminal Activity	8
3.3	Complacency	9
3.4	Perceived Cost	9
4	Security Measures – Systems – Infrastructure	9
4.1	Physical Security	9
4.1.1/2/3/4	External / Internal Barrier	10/12
	Photographs Perimeter Barriers	12
4.1.4/5/6/7	External and Internal Gates	12/14
	Photographs Intrusion / Lighting	14
4.1.8/9/10	Intrusion Protection	15
4.2	Electronic Support Systems	15
4.2.1/2	Lighting	16
4.2.3/4	CCTV	16/17
4.2.5/6	Access Control	17/18
4.2.7	Control Room	19
4.2.8/9	Key Control	19
4.2.10/11	Communication	19/20
	Photographs –Other Aspects	20
4.3	Manpower	21
4.3.1	Personnel	21
4.3.2/3	Security Manpower	22
	Photographs –Other Aspects	23
4.4.4/5	Operations Procedures and Instructions	23
4.4.6/7	Maintenance and Procurement	23
4.8	Other Security Related Aspects	24
	Attachments	25
1	Map Orientation – Regional	25
2	Map Orientation – Greater Area	26
3	Aerial Photographs	27/30
4	Office Organigram	31
5	Incident Summary	32

NOTE: RED FONT INDICATES THE INSERTION OF APPLICABLE TEXT

SECURITY RISK ASSESSMENT
for the
IDENTIFIED RURAL REGION
(A Rural Commercial Farming Community)

AGRICULTURAL OPERATIONS
ABC FARMING COMPANY

Reference: A: ASIS SECURITY RISK ASSESSMENT GUIDELINES

B: AGRICULTURAL OPERATIONS ADMINISTRATION REGS.

C: LEGISLATION, ACTS AND REGS AS APPLICABLE

SECURITY RISK ASSESSMENT

1. INTRODUCTION

The following document sets out the results of the Security Risk Assessment requested by the owner of ABC Farming Company, Mr. A.B. Farmer Owner. Farm Owner

A formal process has been followed in compiling the Assessment to enable easy reference to all relevant information and to facilitate easy updating and expansion of the relevant vulnerabilities and recommendations made.

The Assessment process included references to the processes and procedures as recommended in various international publications.

1.1. Interviews

The following interviews were conducted:

Table with 4 columns: Name, Role, and Conduct Interviews as Required. Rows include B. C. Mperson (SHES Manager), C. D. Nperson (Estate Manager), D. E. Operson (Contract Manager, Security), F. G. Person (Director, Security Response), G. H. Uperson (Workshop Supervisor), and Supt. Gperson (SAPS Local Station).

1.2. The Farm Visit – An actual visit to the Farm during Day and Night.

The Farm Complex was visited during the Day and all relevant aspects inspected and relevant staff interviewed, The staff quarters were also visited and off site infrastructure (pump stations etc.) inspected.

A Night visit should also be conducted in order to objectively assess the Lighting situation and to identify any dark areas that can offer cover for illegal activities.

1.3 Background

A detailed description of the location of the Farm with references to Road designations, distances and natural features.

Include any neighbouring locations that may influence the Assessment.

Describe the buildings that make up the Farm precinct.

Describe the functionality of the various buildings.

Give details of the Family members living in the homestead and personnel that are deployed within the precinct on a routine basis.

Give details of the Farm Labourer's and other farm workers employed on the Farm.

Provide any other information that may be relevant.

1.4 Infrastructure

Describe the detailed construction of the various buildings within the precinct.

The walls; the roof; the windows; the doors; other items such as air conditioning units; details of intrusion protection measures.

Physical security infrastructure, external and internal fences and walls; vehicle and pedestrian gates and access points; perimeter and area lighting; specialist CCTV lighting.

Details of other outbuildings or infrastructure, such as fuel storage tanks, gas bottles for welding and domestic use; external storage of bulk products or farm equipment.

Details of specialist facilities such as Clinic; storage of controlled medicines; cash; electronic office equipment; CCTV recording equipment; computer back-up and servers; communication equipment; electricity infrastructure and standby generators; water supply infrastructure.

Employee change rooms and locker facilities; Employee living units and facilities; Management houses and related infrastructure.

Fire response systems, and early warning equipment and systems. Emergency response equipment and response personnel.

Details of manpower demographics as it may influence the risk and management challenges.

1.5 Mission

The **ABC Farming Company** must protect and secure the safety of its Property, Assets, Information and People from any threat, be it of a direct / active or indirect / passive nature.

1.6 Analysis of the Mission

In order to carry out the Mission successfully, Security measures need to be put into place, amongst others, they will include the following:

- **Physical Security measures:** Walls; Fences; Gates; Security Grill Doors; Burglar Bars etc.
- **Electronic Support Systems:** Electronic Access Control; CCTV, Beams; Passive Sensors; Door and Window Contacts; Metal detection, etc.
- **Lighting:** Area Flood Lights; Exterior Building Lights; Street Lights, Perimeter Lighting; Operations Lighting etc.
- **Manpower:** Security Guards, Security Dogs; Patrol Guards; Control Operators; Surveillance operators etc.

1.7 Restrictions on the Execution:

Response Security services whether they are provided internally by the Company or Private Security Industry are largely reactive by nature. An incident has to occur to which they will then react.

Static security officials posted to access points or on perimeter patrol do present some degree of a deterrent although they are still vulnerable to a concerted armed attack. (Statistics indicate gangs of 4 to 6 armed attackers can be expected should an attack take place)

Report to the Police that some person threatened you and you are concerned for your safety and they will tell you to come back and report when a crime has been committed!!

They can and will only act if a crime has been committed.

Even the electronic support systems are designed to detect and inform when an incident is in progress or has actually occurred.

The only **pro-active elements** of the Security protocols are:

- **Access Control:** You can predetermine who has access to your precinct or not, and in so doing keep out persons of questionable intent.

- Electronic early warning installations provide early warning of an illegal intrusion and permit a pro-active response.
- **CCTV Surveillance:** Behavioral patterns and suspicious behavior can be identified and pro-active response can prevent an incident.

1.8 Integrated Security Measures

To ensure success, Infrastructure, Systems, Manpower and Procedures will have to be put in place and integrated, which will equip the security services to be proactive and to enable them to prevent rather than react to incidents.

1.9 Identification of Tasks

With reference to the mission, the following assigned tasks have been identified.

- Installation of a suitable external perimeter barrier around the farm precinct including access control systems and infrastructure.
- Installation of suitable electronic support systems as identified, CCTV; Detection Beams; Lighting etc.
- Employ applicable security manpower in support of and to enforce the above systems and security measures.
- Enforcement of internal regulations and security procedures with reference to property, assets and personnel.
- Maintain all security infrastructure at 100 % effectiveness at all times.

2 VULNERABILITIES

Economics of scale will obviously dictate the amount of money and when that money can be spent on Security measures.

It is therefore necessary to determine a set of priority vulnerabilities and schedule the installation of the security measures in accordance with this determination.

2.1 Personnel

Identify vulnerable personnel and note their vulnerabilities and how the security measures can protect them and ensure their safety and security while at the work place.

2.2 IT Equipment and Information

Check security measures and procedures to secure the IT equipment and data from unauthorised access. Make sure that back-up systems are secure and actually perform the function for which they are acquired.

2.3 High Controlled and Vulnerable items.

Check that high risk and vulnerable items, such as medicines, electronic cards; and money, are secure and controlled correctly.

Consider the transportation of these items from the source to the farm.

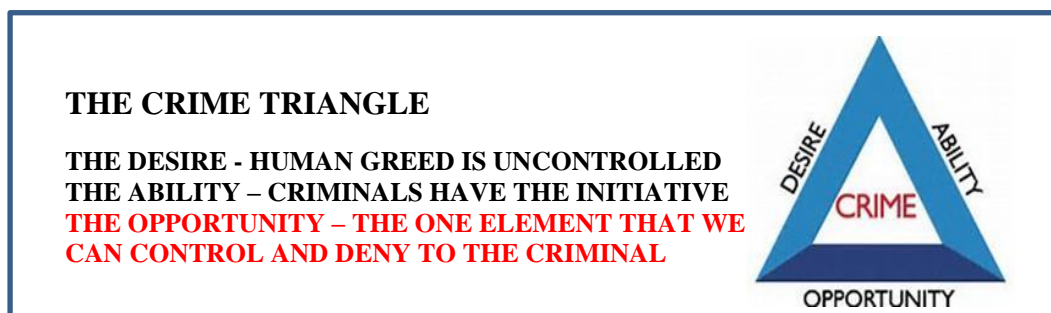
2.4 Other Assets

How are vehicles and mobile farm equipment stored and secured when not in use and parked within or external to the precinct.

Check the stocks of irrigation equipment and other portable farm equipment is secured when not in use.

Remote Pump stations and loading or packing facilities also need to be secured.

Check the security infrastructure in place around personnel quarters that are external to the precinct. The personnel living in these quarters are also vulnerable to attack and need to be adequately protected.



3 THREATS

3.1 Employees

The present Political and Socio-economic situation and climate in the country has seen an explosion in mass action and criminally inspired attacks on commercial and other infrastructure.

There are many scenarios that could trigger the employees to resort to some kind of mass action or criminal activity against the company or its employees.

Further an aggrieved employee who has been disciplined or sanctioned for poor performance or other unbecoming behavior may vent his/her anger by attacking the company personnel or property, or by providing information to other organised criminals who will use the information to attack the people or assets of the Company.

It is a priority that the Complex's security measures be designed with this in mind.

The ability to lock down the facility, provide a safe location for employees, and have an adequate response and support system is required.

Consider the history and social position and previous activities of neighbouring local communities in relation to the Local Authority and more directly the Farm and its people and assets.

An often-volatile situation can occur when the local population has live stock which they herd onto Farm property to graze and in the process damage the farm perimeter fences.

Maintain effective communication with such local communities and their leaders. Address problems at the earliest and lowest level, before they become serious problems.

Recent statistics indicate that a very large percentage of farm attacks are perpetrated either directly or indirectly by dissatisfied ex-employees.

3.2 Criminal Activity

All aspects of criminal activity are on the increase.

Armed robberies perpetrated by armed gangs of as many as 12 persons, are operating in commercial centers, attacking shopping mall stores and stand-alone businesses. Farms are attacked by armed gangs of 4 to 6 members.

The risk is enhanced by the attackers being under the influence of drugs and 'muti', They are ruthless and are known to resort to torture, they have nothing to lose and the farmer cannot rely on accepted values and conscience to protect them.

Not only farm attacks but vehicle hijacking and home invasions accompanied by unmitigated violence are happening with regular monotony and often end in the death or serious injury of the victims.

Electronic equipment remains a priority target and more often than not no one is ever arrested and or the items recovered. Note the recent incidents at the Telkom and Judge's offices. (these are classified as NKP's)

Attacks are no longer random and opportunist. Targets are identified, researched and the attack is well planned and then executed.

The loosely put together physical security measures, the odd CCTV camera and a Security Guard are no longer adequate protection against the modern criminal.

The crime triangle points us always in the direction of the requirement of **denying the criminal the opportunity to attack and or pillage.**

3.3 Complacency

The role of Security officials must be seen and acknowledged as just one element of a whole security effort. Each element should be integrated and compliment the other so that as an integrated whole the Security effort will succeed in protecting and safeguarding the people, property and assets of the ABC Farm Company.

3.4 Perceived Cost

When austerity measures are implemented within the company the first items to come under the knife are Security, Training and Maintenance.

IN FACT THEY SHOULD BE THE LAST !!!

INSERT

**THE ABC FARM COMPANY PRECINCT
AN AERIAL VIEW**

4 SECURITY MEASURES / SYSTEMS / INFRASTRUCTURE –

**THE PRESENT SITUATION IS INDICATED IN OPEN PARAGRAPHS,
WITH PHOTOGRAPHS AS ILLUSTRATIVE SUPPORT.**

**THE DESIRED SITUATION IS INDICATED BY PARAGRAPHS WITHIN A
RED BORDER**

4.1 Physical Security

It goes without saying, that in the present crime and criminal activity climate within which the country finds itself, that any Commercial, Industrial or Farming premises requires adequate and effective access control to its precinct.

Not only is it essential to control the access of persons to the premises, to ensure that only authorised persons have access to the premises, but the reverse is necessary to ensure that company assets both physical and human are protected from injury and or theft and damage.

It is too late when we have to remark “I never thought that they would do that!” or “that it would happen to us”

4.1.1 External Perimeter Barrier

The external physical security barrier.....

Describe in detail the structure, reach, composition and functionality of the external security perimeter barrier. Including gates and electronic security systems.

Where an electric fence is installed refer to Occupational Health and Safety Act (OSHA 1993 Regs.11.6a) as the public have to be protected from accidentally coming into direct contact with the live wires.

4.1.2 External Perimeter Barrier

The External Perimeter Barrier is the first line of protection and the outermost layer of the security effort. All physical security and electronic support systems should be planned and installed in layers from the outermost layer to the final inner layer that protects the heart of Farm (Company).

Physical security measures and supporting electronic support systems are numerous out there in the market place. Make sure that you seek the advise and input of professional security practitioners when you select and purchase your systems. **Beware of the fast talking salesman!**

The layers of security should be planned and scoped to satisfy the basic principles of any security effort, i.e.:

Deter: The visible security infrastructure should send a message to the potential intruder. You are not welcome here!

Detect: Detection beams, CCTV motion detection and numerous other systems can detect an attempt to gain unauthorised access to the Precinct.

Delay: The Physical element of the perimeter barrier should be robust and secure enough to resist attempts to penetrate it, and to delay the attempted intrusion long enough to mobilize a response.

Deny: Ultimately the objective of the security effort is to deny the intruder access to the precinct.

Defend: the security effort should be focused on being able to successfully defend the precinct against an unauthorised intrusion.

Respond: The security plan and layers should be focused on a credible response to any attempted intrusion. Reliable communication and rapid physical response to the scene of capable responders is paramount.

Recover: Any attempted or successful unauthorised intrusion will leave the precinct vulnerable. It is essential that these vulnerabilities whether physical or phycological are addressed, repaired and returned to 100% effectiveness as soon as possible.

An alarm per-se, is not a physical deterrent and only performs as an indicator that the perimeter has been breached. Practice indicates that criminals are not deterred by the sounding of an alarm and will continue with the penetration and criminal activity regardless. They are aware of the response time indicated and act accordingly.

4.1.2 External Perimeter Barrier (Cont.)

Keep the barrier clear of brush and creepers that obstruct a clear view of the barrier and afford hiding space for intruders.

There is always a debate over whether a barrier should be clear view or a solid wall. The decision must satisfy the local situation. If it is desired to keep what is behind the barrier from prying eyes then have a wall, if it is more important to be able to observe who and what is going on outside your barrier then install clear view.

i.e. The Precinct is situated in a rural area, surrounded by cane fields with no like premises or neighbours in the vicinity. This means that there is no support or protection readily available other than that created by the Farm itself.

Robust effective barrier will immediately portray an image of order and control and will be a major deterrent to any planned intrusion.

4.1.3 Internal Fencing

Describe in detail the structure, reach, composition and functionality of any internal security barrier.

These would normally be utilised to indicate and separate various internal facilities from the main open space within the precinct and the facilities. i.e. Vehicle Park; Bulk storage of Fuel & Fertilizer; Chemicals and insecticides; Scrap yard; Stores with external storage area; irrigation equipment; electricity and water infrastructure; Clinic; administration offices; residential units; etc. etc.

4.1.4 Internal Fencing

The principals discussed above are all valid and can apply to the inner fencing to a greater or lesser degree. This will depend on the value of the infrastructure protected and or the importance related to the overall security of the precinct. This is the second layer of security and may contribute considerably to the over all security of the precinct.

When planning additional security elements, it is good financial practice to prioritize different elements and phase them in over a reasonable period to allow for financial budgeting and procurement protocols.

PERIMETER BARRIERS

Insert photographs of the existing security infrastructure. These will illustrate any vulnerabilities and weakness on the perimeter that can be used to motivate the additional effort required or planned.

External Security Barrier

2nd view External Security Barrier

Vulnerable Sections of the External Security Barrier

Access Gate (view from outside)

Access Gate (view from inside)

Internal Fencing

Examples of the various Installations

Others as required.

THE DESIRED SITUATION IS INDICATED WITHIN THE RED BORDERS

4.1.5 External Perimeter Gate

The number of gates in the external perimeter should be limited to the absolute minimum required to ensure the effective functioning of the precinct. Gates by their very nature create a weak spot in the perimeter.

As with the perimeter barrier there are numerous solutions and systems available on the market. The owner must select the best and most economical solution to achieve the desired result at his precinct.

Pedestrians should not gain access through the vehicle access gate. Install a pedestrian turnstile to the side of the vehicle gate or at another suitable location. Remember that during peak access/egress periods the turnstile should be supported by a security official.

4.1.6 External Perimeter Gate

The main vehicle access gate should be a robust heavy duty sliding gate, with at least a metal frame, which should also be automated. The gate requires substantial pillars to support it effectively.

An electronic intrusion detection beam is recommended. The beam carriers can be mounted on the gate pillars. The beam must be linked to the internal alarm system.

It is also recommended that a gate electric actuator be installed to accommodate a proximity card reader and that each authorised employee be issued with an individually coded card. (**refer- Access Control**)

The gate remains the critical access point, it should be kept in the closed position at all times, and opened only electrically or on demand. After hours the gate should be locked with a high security padlock which will prevent it being forced off its rail and the electric motor being bypassed.

Ideally, if the location and finance permit, the gate should be constructed with a double-gate vacuum system. This permits the vehicle wishing to access the precinct to enter the first gate while the second is still closed, and the second is only opened, when the first is closed, and the access route is secure.

The Security official posted at the gate is still responsible to oversee the access control and to implement any searching or alcohol testing required. A detailed post instruction must be written for the post.

The Security Guard should be provided with a substantial guard hut that will provide protection from small arms fire and allow the guard time to raise the alarm and secure back-up, should the precinct be attacked. The Guard hut can be back from the gate in a position to permit observation and control, but out of the direct line of fire.

4.1.7 Internal Perimeter Gates

Internal gates are as important as the external perimeter barrier gates. In some respects even more so, as they control access to identified critical and vulnerable resources.

Describe in detail the various gates and the resources that are protected and secured by these.

Take photographs that highlight any weaknesses and infrastructure that requires attention.

Insert photographs of internal installations and resources. These will illustrate any vulnerabilities and weaknesses that can be used to motivate the additional security infrastructure and systems required.

LIGHTING AND INTRUSION

Bulk Stores

Vehicle Parks

Workshops

Etc. Etc.

4.1.8 Internal Gates

The gates should present the impression of being a solid effective barrier to an intruder.

It would be an advantage to automate any of the gates that are situated in a position that can accommodate the electric motor and activation mechanism.

Getting out of a vehicle to open and close a gate exposes the driver to attack and is a situation to be avoided.

Ensure that locking mechanisms are of a high quality, are pick resistant and have a bolt cutter resistant steel shackle. (refer Key Control)

4.1.9 Intrusion Protection

Provide details of burglary guards and grill doors fitted to windows and doors.

Provide details of vulnerable areas such as air conditioning units, roof vents fire escape doors and any other possible intrusion locations.

All padlocks utilised must be at least of security level 3 and of high quality. Review the quality of the padlocks in use and the key control procedures and authorities.

The routines and procedures regarding status of doors and grills (when locked or not) is important and requires formalization

Record the status of the internal intrusion alarm, fire detection and smoke alarm system.

Evaluate the possibility of linking the intrusion and fire alarm system to your neighbours, the local authority emergency control room or the local SAPS station.

4.1.10 Intrusion Protection

Every window or aperture that provides access to the interior of an office, store or other location containing resources and equipment, should be protected by the fitting of professionally designed and scoped intrusion prevention bars. Bars should be cemented into the wall surrounding the aperture and not just screwed into the window frame.

All doors and other pedestrian access points should be protected by steel grill doors, with slam locks and bolts into the wall above and floor below. The bolts should be padlocked with level 3 security locks of high quality.

It is necessary to determine an open, verses, locked procedure and routine for all the offices, stores and controlled spaces in the Precinct.

The intrusion detection alarm system should include passive intrusion sensors in all the controlled locations including the Manager's homestead.

Install intrusion beams across the established access route and internal gates providing access to the Manager's homestead.

Include fixed and portable panic buttons in the design of the system.

Include a remote indicator panel in the Manager's homestead.

A system to control access of visitors and contractors is required. An appointment needs to be made and a register completed. Visitors must be met by the host and not be allowed to walk around the precinct on their own.

Designate a parking area for visitors and contractor vehicles outside the perimeter of the workshop and operations area.

Consider keeping a team of two dogs at the Managers Homestead, one large and one small (yapper). The dogs to be kept inside at night.

4.2 Electronic Support Systems

4.2.1 Lighting

Record details of all exterior lighting as it affects visibility after hours in the precinct. Lighting can be classified as standard building lighting, for passages, walkways etc., specialized lighting for a work area or loading platform, perimeter lighting, CCTV lighting and general area flood lighting. Interior office lighting as necessary to provide adequate lighting for the office workers.

i.e.: As the estate is surrounded by agricultural land, there is no ambient lighting in the area. This affects the general level of illumination within the general area of the precinct.

4.2.2 Lighting

Perform a detailed review of the lighting installation and identify any vulnerable dark areas, particularly around the precinct operating areas the living units and the manager's homestead.

Install or reposition the required lighting to address the identified areas.

The main vehicle gate area should have flood lights linked to the alarm system to create a shock effect.

If CCTV is considered then it is essential that the CCTV cameras are directly supported by effective lighting units.

Perimeter lighting should be positioned inside the perimeter barrier and should face outwards beyond the barrier line.

4.2.3 CCTV

Review the positioning of each existing or proposed CCTV camera.

The camera should be given a task just as you would give an instruction and tasks to a security official. Position of the camera is critical. The resultant image must be a high quality resolution and images must be clear and usable as evidence. Persons recorded must be identifiable and images must be usable as evidence in a Court of law.

As mentioned above there are numerous Electronic systems out there in the market place. Professional advice should be obtained when making a purchase. The CCTV system must have a defined objective and should be purchased and installed to achieve this.

Insert photographs of lighting and CCTV installations and resources. These will illustrate any vulnerabilities and weaknesses that can be used to motivate the additional security infrastructure and systems required.

GENERAL EXTERNAL OPERATING AREAS

Bulk Stores

Vehicle Parks

Workshops

Barriers and Gates

Etc. Etc.

4.2.4 CCTV

A top of the range system at present will include Thermal- (heat detection) motion detection cameras with recording and alarm linked protocols.

As a general illustration below is a cost effective system of 6 cameras, with a recording capability. This should be adequate to secure a small precinct. Cameras are proposed in the following positions.

1. The Main gate: Camera to view number plate and driver.
2. The Main office and Admin Offices: Camera to view person/persons standing in front of the door and along the veranda.
3. The Clinic entrance: Camera to view persons standing in front of the door and in the waiting area.
4. The Main workshop general work area: Camera to view the general work area with emphasis on the working space.
5. Main Stores: Camera to view the main controlled stores door and Oxy –Acetylene gas bottle cage. .
6. Vehicle Yard: Camera to view the Dieseline bulk tank and bowser. Include vehicle number plate in the view.

The recording unit must be in a secure location where it cannot be compromised by any unauthorised persons. Remote monitors can be provided in the GM office and the main Admin office. Modern systems can also be linked to the Cell phone network for management off-site monitoring and response.

It is essential that the type and location of the Cameras installed can provide the critical images required to secure the precinct.

Camera housings, the recording unit and any cable junction boxes should be connected to the alarm system to prevent tampering.

4.2.5 Access Control

Provide details of the access control procedures and protocols in place at the precinct.

**Is there an electronic access card system?
Are all employees issued with a photo ID card?
Is the card worn on the person and visible at all times?**

Is there a control system for visitors and contractors?

**Is a record kept of all vehicles that enter the precinct?
Is there a gate pass system to control movement of vehicles and equipment leaving the precinct.**

Is there a alcohol testing procedure and a searching procedure.

Are the COVID 19 protocols in place and strictly followed

4.2.6 Access Control

There are numerous proximity and smart card systems available on the market. These have also now been enhanced by the development of Biometric systems.

The choice should be informed by the value of the assets to be protected and the priority placed on keeping unauthorised persons off the premises and out of the precinct.

As a very minimum the Farm personnel should all be issued with Photo ID cards.

Additions to this system to enhance the security at the precinct can be the following.

An electronic access control system for the precinct:

1. Separate proximity disc or embedded card to control the access through the main gate.
2. Access readers on the Managers office door.
3. Access readers on the Admin offices.
4. Access readers on the main access to the Clinic.
5. Access readers on the controlled store and other high priority locations.

Authorised vehicles should have a windscreen disc indicating the vehicle status and registration number.

The main access gate should be a robust heavy duty sliding gate, which should also be automated. The gate requires substantial pillars to support it. An electronic intrusion detection beam across the road way , is however recommended. The beam carriers can be mounted on the gate pillars. The beam must be linked to the internal alarm system.

An identification and registration system is required to control the access of Visitors and Contractors.

Apply a referral system to control access to the Clinic. The procedure and application should be reviewed to ensure that it cannot be manipulated.

It is worth considering fencing the Clinic and other selected and vulnerable areas, off from the rest of the workshop and vehicle yard with provision for a separate pedestrian turnstile adjacent to the back of the main store building.

This gate should include an electronic lock and CCTV Camera.

Refer to 'Manpower' for further proposals.

4.2.7 Control Room

The precinct has no Control room facilities.

Cell phone and Two Way Radio linked to the Security service provider serves as emergency callout and activate the armed response vehicle.

4.2.8 Control Room

A control room is an expensive installation to create and even more expensive to maintain the function.

It makes sense for a regional community to maintain a regional control room / center that serves as an early warning and response control and co-ordination center for the whole community.

Modern Radio technology makes this a practical and cost effective arrangement.

4.2.9 Key Control

There is no formal key control procedure or key management.

4.2.10 Key Control

It is essential that there is a key control procedure in place.

Duplicate keys must be kept in a lockable key box.

Keys must be marked with location and appropriate security ratings (red, yellow, green) and have linked authority levels for issuing.

Personnel must sign for original keys issued to them, and they remain responsible for the security of the location that they control.

4.2.11 Communication

Evaluate and review the communication system in use at the precinct and the network available within the region as a whole.

Fast, secure and reliable communication can literally mean the difference between life and death.

What communication system is available and in use by Management and personnel at the precinct. Is the local Cell phone facility available and reliable? Do key personnel have official company phones?

Is there a security service provider who provides an armed response and fence patrol officials? Do they have a 2-way radio system between the response vehicle and their control room as well as cell phones for back-up. How reliable and effective is it, does it cover the whole region or are there dead spots with no reception?

4.2.12 Communication

Relying on a single mode of Communication is not ideal. It is suggested that an additional 2 cell phones with an alternate service provider be acquired and deployed 1 with the Manager and 1 with the Complex Admin Office.

For security peace of mind, however, a radio base station should be obtained from the Security service provider and linked to the armed response Vehicle and the Security control room.

The Alarm system should be expanded to include panic buttons linked to the Security control room and selected Cell phones.

Buttons should be installed at least as follows:

1. Managers Office; 2 Main Admin office; 3 Clinic;
- 4 Main Gate; 5 Workshops.

Key personnel have Cell phone communication and most employees have their own private Cell phones which can be used in an emergency.

Insert photographs of any other areas or locations that have a security or safety influence within or off-sight of the precinct. These will illustrate any vulnerabilities and weaknesses that can be used to motivate the additional security infrastructure and systems required.

OTHER SECURITY / SAFETY ASPECTS

Stores

Vehicle Parks

Workshops

Employee Quarters

Remote Pump Stations

Equipment Storage

Scrap Storage

Etc. Etc.

4.3 Manpower

4.3.1 Personnel

The Personnel do not have ABC Company Identification badges which indicate their employment with the company.

Access control by any electronic system or Security officer is extremely difficult in the absence of any form of Identity Card control system. (Refer Access Control)

4.3.2 Security Manpower

It is critically important to assess in detail the whole internal and external characteristics of the precinct and its contents. Identify the areas, locations, resources and people that are vulnerable. Evaluate and identify the protection measures that can be installed and crated in order to adequately protect and safeguard these.

Assuming that the aforesaid aspects and measures have been correctly and effectively addressed it is now time to determine which of the physical or electronic security measures in place require the physical presence of manpower, a security official, in order to be fully functional and effective.

Systems have no discretion, and no capacity for reasoning when confronted with a unusual or out of the ordinary situation. In such a situation it may be necessary to deploy a human to bridge the gap and ensure that the systems all function in an integrated manner in order to achieve the desired result.

One security official at the access gate cannot prevent the full-frontal attack of an armed gang. But if he has the correct infrastructure and resources he can secure the precinct, raise the alarm and monitor activities from a safe location, while back-up is on the way.

Manpower is expensive, which makes it all the more essential that the correct person, is deployed at the correct time, at the correct place, and equipped with the correct resources in order to protect the precinct its people and assets.

Where is the local Polices station, where is the nearest neighbour, how long will it take for a response to the panic button. The precinct managers plans and protection measures have to be deployed and prepared to secure the precinct until back-up can arrive. Can they hold out for 15 to 20 minutes??

First response plans need to be well thought out and recorded in detail. Who does what, when, where and what are the desired results.

Police and armed response all drive like hell to the scene !!! After the event !!! Ambulances, yes and crime scene investigators, yes. Others no!! Allocated responders must go to predetermined cut-off points, get ahead of the attackers and wait for them to come to them!!!

4.3.3 Security Manpower

Electronic Security systems are only as good as the manpower available to back them up. Systems have no discretion, cannot be flexible and cannot adapt responses to a changing situation.

A TYPICAL PROPOSAL

As a minimum it is recommended that two security officials be deployed 24/7 at the precinct .

1. During office hours one official will be posted at the Main gate. He/she will man the gate and enforce access control. Personnel once issued with Access cards will open the Gate (boom) themselves and the security official will provide support. The official will open for visitors and contractors and will complete the applicable registers. He will also control parking.
2. The second official will patrol the perimeter with particular attention given to the clinic, especially when high numbers of patients are in attendance.
3. After hours the gate will be locked closed and both officials will patrol the Complex's fence line and inner environs, including the Manager's homestead.
4. The officials must operate in such a manner that they are a back-up for each other in the event of an attack or attempted intrusion.
5. The Main gate should be kept closed after hours and closed by the official at any indication of an unusual event or approach.

Routines must be formalized and provide for a relief system and swopping of roles at least every 2 hours.

The officials must be equipped with:

- 1 Uniform and insignia, including Cold weather and Rain wear.
- 2 Two way radio for self-communication.
- 3 Cell phone for external communication to Management and Response vehicle.
- 4 Panic Button for communication to the Security 4U control room and response vehicle.
- 5 Tonfa Baton, Pepper spray, Hand-cuffs, re-chargeable torch.
- 6 Pen, pocket book, emergency call out list,

Armed guards are not recommended due to the isolation of the precinct and the target that the fire arm itself may present.

The provision of a safe place / location in which, and from which a security official can raise the alarm and secure back-up is critical. A security official cannot be expected to repulse or even successfully

Insert photographs of any other areas or locations that have a security or safety influence within or off-sight of the precinct. These will illustrate any vulnerabilities and weaknesses that can be used to motivate the additional security infrastructure and systems required.

OTHER SECURITY / SAFETY ASPECTS

Electricity Infrastructure

Electricity External Feed (Eskom)

Water Supply Infrastructure

4.4 Operating Procedures and Instructions

The security measures can only be effective if they are properly regulated by detailed procedures and instructions.

4.5 Operating Procedures and Instructions

Write a standard operating procedure (SOP) for the locking up and unlocking of the Complex on a daily basis including status of various controlled locations during the working day.

Review and update emergency procedures, fire response and First aid response. Appoint Evacuation, First aid and Fire Marshalls in terms of the OHSA.

Compile an Alcohol testing and control Policy for the Complex.

Compile a search policy and procedure for the complex. Determine the need for the use of metal detectors at the Complex.

Compile duty sheets and post instructions for the Security officials and Wardens.

4.6 Maintenance and Procurement

Maintenance of all security related equipment and systems is essential to ensure that all elements function continuously as designed and are fit for purpose 24/7.

Security systems and infrastructure are planned and installed based on 100% performance 24/7, any breakdown or mal-function immediately compromises the Security of the Complex.

4.7 Maintenance and Procurement

Ensure that the Procurement procedures and contracts with suppliers allow for priority call out and immediate repair of Security systems and infrastructure.

4.8 Other Security Related Aspects that may be encountered at a typical location or precinct.

4.8.1 Information / Prohibitive Signage

Existing signage is faded and signs are in a poor condition. This exhibits a negative image and lack of order and control.

Additional signage indicating the use of CCTV cameras and prohibition related to access etc. should be added.

4.8.2 Community Communication

The Management must establish Communication forums with the local tribal chiefs and local SAPS station Commanders. Meet the SAPS Cluster Commander (Brig. Zundi - Eshowe) for coffee or a beer occasionally.

The Community must accept ownership of projects and be informed of pending changes or new activities on the Estate. This will enable Community buy-in and less conflict.

4.8.3 The Control of dieseline theft and other estate incidents; cattle fence vandalism and theft; cane theft; Illegal cattle grazing; irrigation equipment theft and vandalism and staff quarters theft; are outside the mandate of this Assessment, but it is obvious from the recorded incidents that something has to be done to at least curb and reduce these incidents.

4.8.4 The Clinic Sister should not travel alone to the Estate. Her routine is known and she is in possession of valuable commodities.

4.8.5 Due to poor response and investigative capacity from the SAPS, private investigations run in parallel to the SAPS and compilation of a parallel docket could bring significant results and increase the chance for successful prosecutions.

4.8.6 There is no Standby generator which indicates that the Complex is in total darkness and all electric / electronic systems are down, in the event of a power failure. Critical electronic systems can work off UPS back-up for a short period but lighting and other systems require Generator power.

4.8.7 A “safe room” should be established within the Managers Homestead where he and his family can take refuge and be safe during a home invasion. The room to be secure from the inside and fitted with a solid secure door. Provide for effective reliable Communication, to call for response back-up. Provide water and other refreshments.

ATTACHMENTS

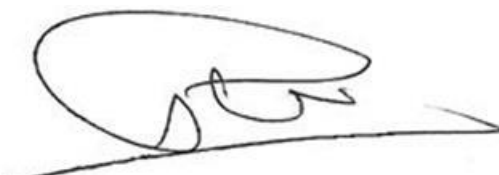
The following maps, drawings and documents should be attached to complete the assessment.

They are available as supporting motivation to the assessment as a whole.

- 1. Map orientation of the selected Region**
- 2. Map orientation of the selected region within the greater area.**
- 3. Ariel photographs as appropriate.**
- 4. ABC Company organisation and personnel structure**
- 5. Incident History – by Month, and year on year**

This is a comprehensive template based on years of experience in protecting rural communities, however, there are too many variables in each situation to include every possibility and option. The author therefore advises communities to use this template as a starting point and modify it to their particular environment, refreshing the assessment annually.

**LAURENCE PALMER
LP CONSULTANT
unicornnlpconsulting@gmail.com
October 2021**



COPYRIGHT AND DISCLAIMER APPLY