Leadership and Governance

MPS 1 – Leadership

Intent

To set clear expectations for Security Management that are codified with a policy and supporting procedures which are consistently applied by leaders at all levels.

Required Actions

1.1 A Security Policy signed by the most senior executive for The Company - applicable to both Karowe Diamond Mine (KDM) and the Corporate Office at the Diamond Technology Park (DTP) should be prominently displayed. This display, subject to the location (at the Corporate Office or KDM) should be either communicated via email and placed on available and accessible social media platforms like Yammer. For KDM, this should be placed for viewing by staff, contractors and visitors on entry to the facility (Blue Gate at the Personnel Control Centre/PCC) and on entry to the process plant and recovery building or diamond handling area.

1.2 The Security Policy will be a short document that will at least outline ’s obligations and the individual’s obligations regarding Security and/or security related activities.

1.3 The Policy will be incorporated into the operation’s induction process for all personnel, contractors and visitors. A process will exist for recording that all personnel, contractors and visitors understand and agree to comply with it.

1.4 The Heads of Department / HODs, Superintendents, etc. - leaders at all levels - will endeavour to make the Security Policy relevant to their place of operation / workplace.

1.4.1 Through setting a limited number of Golden Rules that define applicable security requirements based on the associated risk profile and acceptable risk tolerance

1.4.2 Through short awareness and training sessions on aspects of Security conducted at least bi-weekly or as often as security incidents and matters are brought to their attention.

1.5 Where possible and applicable, specific Security accountabilities and performance measures will be documented within role descriptions for those in high-risk diamond areas, security and management.
(*Note: Within the current Performance Management Scorecard/System’s and approved Generic Objectives, reference is made to ‘Security’ and ‘Governance’ where KPA/Objectives and KPI/Measures are listed for those in a HOD and/or Superintendent role. Consultation will need to be held with HR to review any role descriptions for those in high-risk diamond areas / Security / Management and determine if additional security responsibilities are required to be included and/or enhanced*)

1.6 Leadership teams in high-risk diamond areas will regularly assess the Security culture and adherence to security protocols of their workplaces. This is especially important during high risk / high exposure activities that are undertaken during maintenance, shutdowns, clearing of blockages/spillages, etc., to name a few.

MPS 2 - Chain of Custody and Security Control Committee

Intent

To provide clear accountability for the custody of diamond material from the ore body to the point of onward shipping to the customer – this is the chain of custody.

Required Actions

2.1 The chain of custody for each operation will be set out in matrix form, with an accountable manager named for each part of the chain and any security or controls for which they are accountable listed underneath their name. Do find annexed, The Company's Chain of Custody Matrix as Annex D.

2.2 To indicate all accountable and responsible people, the Chain of Custody Matrix does list all those from the MD, GM to those in the Mining Operations and Support Services, have been included in the chain of custody where appropriate.

2.3 The chain of custody document will be reviewed at least annually and in the event of any personnel or process changes.

2.4 The managers in the chain of custody will be accountable for the effective delivery of Security in their area of control including the safety and security of personnel, property, product and reputation and form the basis of the Security Control Committee (SCC).

2.5 Security roles and responsibilities are to be clearly defined and presented in the form of a RACI chart. Do find annexed, The Company's RACI Chart that outlines those accountable and responsible for the Minimum Performance Standards as contained in the Company Security Control Standard, as Annex E.

2.6 The SCC, which will have responsibility for ensuring that an effective Security programme is established and integrated into each operation's work, will be chaired by the most senior executive of the business or operation.

2.7 The SCC will have a clear mandate and charter, The Company's Security Control Charter, as Annex E, endorsed by the MD of The Company and the most senior executive of the operation. As a minimum this will include (but not be limited to):

2.7.1 Developing and approving joint operations and security procedures in high-risk areas,

2.7.2 A focus on eliminating spillage, blockages or requirements for unscheduled maintenance that provide opportunity for hands on exposure to concentrated diamond product and identifying the root cause of each,

2.7.3 Reviewing the human aspects of the teams working in high-risk areas. Such reviews might look at the recruitment into the teams, the quality of leadership, spans of control, quality of training, process discipline and other aspects of workplace culture.

2.7.4 Review data and product quality indicators as possible indicators of loss.

2.7.5 Providing guidance for Security inquiries and Serious Incident Reviews, authorising and monitoring the implementation of the resulting action plans

2.7.6 Assessing incentive schemes and measures for their impact on Security.

2.7.7 Reviewing security department policies and procedures and performance against security metrics, 2.7.8 Review and approval of facility design changes for adequate Security measures.

2.8 The SCC will meet at least four times a year. Minutes will be taken of these meetings, actions agreed, decisions recorded, and individuals made accountable for their delivery.

Guidance

- The SCC is designed to be deliberately cross functional and an open and transparent committee.
- It is a change mechanism that will allow managers to hold their peers to account and ask questions of performance.
- Where possible it should be aligned with other change initiatives at the operation, particularly quality improvements, or interventions by human resources.
- Particularly important to include as chain of custody owners are the process managers, Geologists, and the Risk Manager: Security involved in the high security risk areas of a business' operations.
- Operations may spread the duties of the SCC between two tiers:
    - The Operation's SCC consisting of Heads of Department (HoD) or senior managers meeting at least quarterly, and
    - Operational supervisors focused on the detail of Security in diamond areas, the development of joint procedures and the management of change.

MPS 3 - Separation of Duties

Intent

To reduce the risks of error and fraud by dividing or allocating tasks among various individuals.

Required Actions

3.1 In handling and accounting for diamonds, operations will seek to give a single individual responsibility for only one of the following four components: custody of diamonds or diamond data, authorisations, record keeping, and reconciliation.[1] This will be evident in the way diamonds are handled and secured and how data on them is recorded and stored.

3.2 In the execution of security duties operations will seek to ensure the separation of duties between Security Operations, Technical Security Systems provisioning and Investigations. It is best practice to have independent oversight and assurance over diamond handling activities and technical security systems.

3.3 The security function will be organisationally distinct from the operational management of the diamond recovery or diamond handling process. Currently, at The Company, the Security Department operates and reports separately from the operational management of the four components as listed in 3.1 above.

3.4 Security personnel will not be involved in the process or operational management of diamond areas.

3.5 The Company will have a person designated as the 'Risk Manager: Security (Security Manager)' who is responsible for security operations at both Karowe Diamond Mine and Diamond Technology Park / DTP (Corporate Office. The Risk Manager: Security is supported by the Karowe Mine (upstream) Risk Co-Ordinator (Security Superintendent), the Gaborone (downstream) Risk Co-Ordinator (Security Superintendent) and the Risk Co-Ordinator Operational Support (both KDM and DTP).

3.6 The Risk Manager: Security is the person who will be accountable for the delivery of security at the operations (both KDM and DTP) and co-ordination of security on behalf of the General Manager in accordance with this standard, laws rules and regulations and applicable The Company Policies.

3.7 The Risk Manager: Security will report independently and directly to the most senior executive of the operation. Currently, the Risk Manager: Security reports direct to the Chief Risk Officer, who reports to the Managing Director.

3.8 The Risk Manager: Security will have regular interaction with the most senior executive of the operation. This will be not less than twice monthly.

3.9 The Risk Manager: Security will support Heads of Department (HOD) / Business Unit Managers in achieving Security in their areas through enforcing the intent of this standard. Where a HOD wishes to deviate from this standard the Risk Manager: Security Manager will escalate the issue to the SCC or the General Manager or MD The Company.

3.10 The Risk Manager: Security will use metrics to improve security effectiveness and report on performance against them to the SCC.

[2] Based on COSO guidance for segregation of duties: www.coso.org

3.11 There will be a complete and current/ up-to-date security procedures and post orders in place for all roles, as defined by the review dates. These will be available for the security officers to reference.

3.12 Where the Risk Manager: Security has other roles, like that of legally appointed Airport / Airstrip Manager (per the Civil Aviation Authority of Botswana / CAAB), it is noted that majority of the time should be spent on Security issues.

Guidance – Reserved

MPS 4 - Risk Management

Intent

To ensure that we focus our efforts and resources on the greatest risks; we identify, evaluate and control risks using a common The Company risk management approach, which is well understood. See guidance below.

Required Actions

4.1 The Company has formulated and adopted a Risk Management Policy and Framework.

4.2 The E*nterprise Risk Management (ERM) Policy* outlines The Company's risk management process and sets out the responsibilities of the Board of Directors (the Board), the Audit and Risk Committee (ARC), the Managing Director (MD), Executive Management and staff members within in relation to risk management.

4.3 The *ERM Policy* should be read in conjunction with the *The Company Enterprise Risk Management Framework* for detailed explanations.

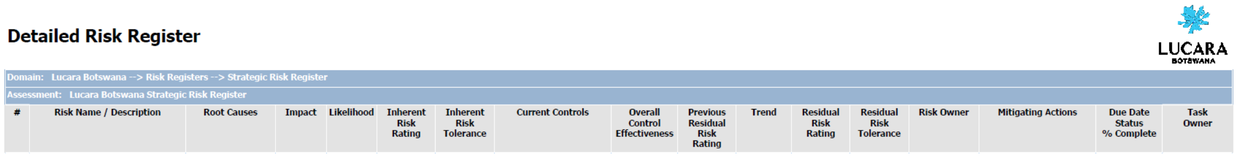
4.4 The ERM Policy and Framework should serve as the basis for Security Risk Management assessments and associated risk considerations, whilst additionally taking into account other leading security and mining risk management practices documents.

4.5 All personnel should utilise existing risk processes like daily task risk assessments, planned task observations (PTO's), root cause analysis (RCA's) and other associated software like CURA (ERM), Perspective (Security Incident Management) and Isometrix (SHE Incident Management) to be able to assess and manage risk at the respective task, activity or facility level.

4.6 The basic format and structure of risk registers will be consistent as defined in the ERM Framework and Policy and as underpinned within the CURA platform for all operational and strategic related risk registers. These risk registers will take into account the following risk management matrix and register template sections:
- Risk Impact Rating
- Likelihood / Probability Rating
- Control Effectiveness
- Speed of Onset
- Risk Trending
- Risk Tolerance
- Risk Response

4.7 See examples below of risk registers outline

Risk #	Risk Description	Root Cause	(I)	(L)	Inherent Risk (IR) (Formula) (I) x (L)	Inherent Risk Tolerance	Controls/ Mitigation plans in place	Control Effectiveness (CE)	Residual Risk Rating (Formula) (CE X IR)	Residual Risk Tolerance	Risk Owner	Risk Response	Risk Trending	Speed of onset	Mitigating Actions



Detailed Risk Register

LUCARA BOTSWANA

Domain: Lucara Botswana --> Risk Registers --> Strategic Risk Register

Assessment: Lucara Botswana Strategic Risk Register

#	Risk Name / Description	Root Causes	Impact	Likelihood	Inherent Risk Rating	Inherent Risk Tolerance	Current Controls	Overall Control Effectiveness	Previous Residual Risk Rating	Trend	Residual Risk Rating	Residual Risk Tolerance	Risk Owner	Mitigating Actions	Due Date Status % Complete	Task Owner

4.8 Controls or action plans will be developed to manage Security risks to as low as reasonably practical (ALARP).

4.9 Risk registers will be current and regularly reviewed.

4.10 The status of all high and very high risks will be reviewed and updated at least annually to ensure that the controls are still relevant, applicable and executed as per requirement

4.11 Critical Controls will be identified for high and very high risks in diamond areas and will be resourced to be effective in mitigating the risks and remain resilient to disruption.

Guidance

- The main guidance is derived from:
  - ISO 31000
    - Internationally, this is the main standard that drives risk management in all domains, whether safety risk management, financial risk management, operational risk management or security risk management (There may be many more).
  - The MIRM (Mineral Industry Risk Management Framework):
    - The MIRM is a process that was designed and commissioned between companies form the extracting industries and the University of Brisbane in Australia, and is largely used to inform risk management, especially in the safety domain.
  - NIST (National Institute for Standards and Technology:
    - Security risk assessments are unique in the sense that most of the threats we are faced with are adversarial in nature. In order to understand this type of threat and how it operates, we are guided by the NIST risk management framework.
  - The concepts of ORM (Operational Risk Management):
    - ORM or Operational Risk Management provides guidance to understand the way in which risk management is to be applied by following an integrated approach, thereby ensuring that risk is mitigated at all levels within the organisation.
  - The diamond security philosophy:
    - In diamond security and loss prevention, a unique philosophy was designed and developed over the years that has proven itself beyond reasonable doubt. A thorough understanding of this provides guidance especially in understanding the security control environment.
  - security policies and procedures:
    - Each company has a unique set of security and related policies and procedures that must be incorporated into the risk management strategy.

MPS 5 - Legal and Regulatory Requirements

Intent

To ensure that legal obligations and requirements set the minimum standards for how The Company operates and that The Company complies with all legal, regulatory, and other associated requirements, including but not limited to The Company, The Company Pty Ltd and Karowe Mine internal policies, standards and public commitments.

The Company needs to demonstrate their commitment to ensuring and maintaining compliance to laws and regulations (current and future laws and regulations) as a responsible corporate citizen in terms of good corporate governance.

The Company - with a producing mine (Karowe Mine) and exploration licenses in Botswana - is a 100% owned Canadian diamond mining company, falling under the The Company Diamond Corporation structure. The Company is a member of the Lundin Group of Companies and is listed on the TSX, Nasdaq Stockholm and the Botswana Stock Exchange under the symbol "LUC".

With a local presence and active operation in Botswana, but with international company holdings, The Company will be subject to both local and international laws, rules and regulations. This requires a view of the regulatory landscape and achieving compliance to be far wider than just being Botswana-focussed. Considerations of intra/extra jurisdictional aspects and their applicability needs to be part of how The Company reviews the legal and regulatory requirements.

For example, reference to the UN Global Compact, OECD Guidelines, Natural Jewellery Council, Kimberlite Process, Voluntary Principles of Security and Human Rights (VPSHR), Towards Sustainable Mining (TSM), Responsible Jewellery Council (RJC) and UN Sustainable Development Goals, etc., to name a few are those that will impact The Company ability to ensure compliance is maintained for those over-arching practices / guidelines that has been committed to by the holding company in The Company Diamond Corporation.

Required Actions

5.1 Each operating site (Karowe Diamond Mine and the Gaborone Corporate Office) will implement and maintain a process that systematically identifies, registers, updates and assigns both general and specific external legal and regulatory requirements. These requirements will be based on organisational position within The Company as per legal appointment, as per position as the Head of Department and/or as the appointed Risk / Compliance Champion.

5.2 A legal register or similar document should be centrally available and accessible that serves to account for all applicable statutes that are required for The Company to adhere to on an ongoing basis as a mining company. This should include those statutes that may be triggered by an event/activity/occurrence that are not listed specifically in the legal register.

5.3 There will be periodic checks by the legal appointee / Head of Department / appointed Risk / Compliance Champion to determine their operational understanding of the external legal/statutory requirements. Furthermore, they are to ensure that the legislation being referred to and applicable to their area of operation, is current and that their inputs to assess, update and attain compliance thereto, is being maintained to the required standards for audit and monitoring purposes.

5.4 Legal and other requirements will inform associated direct or ancillary work processes that may need to be communicated appropriately to relevant employees and/or contractors.

Guidance - Reserved

Process Integrity

MPS 6 – Quality Assurance and Process Integrity

Intent

To ensure that the orebody is understood such that operational processes and protection standards can be adjusted appropriately to maximise revenue recovery. To ensure operational processes are in control and measured so that variations in expected production and revenue recovery provide triggers for increased security and managerial focus on areas, activities, or people.

Required Actions

Diamond Liberation

Granulometry

6.1 Establish In-Situ Diamond Size Frequency Distributions (DSFD) - Diamond Footprints per facie/source

6.2 Establish In-Situ DSFD - Revenue Distributions per facie/source

6.3 Establish In-Situ DSFD - strive for total content curve but at least finer than expected bottom cut-off size to ensure optimisation of revenue recovery

6.4 Establish In-Situ DSFD - Use Diamond Footprints and Revenue Distributions per facie/source to determine liberation requirements

6.5 Granulometry analysis will be applied to liberation. The trade-off between revenue liberation vs. diamond damage will be considered

Modelling

6.6 Implement process modelling to determine optimum liberation circuit design (e.g., LIMN, JKSimMet).

6.7 Determine settings and operating parameters specific to liberation equipment to optimise liberation

Blasting

6.8 Blasting parameters will be optimised and applied to maximise liberation but minimise damage (blasting cheaper than plant comminution processes).

Monitoring and Assessment

6.9 Evaluate liberation performance and trends monthly

6.10 Ensure routine equipment monitoring and assessment is in place and corrective action taken as appropriate (crusher gaps, screening efficiencies, etc.)

6.11 Ad hoc sampling and assessment of all coarse tailings will be conducted to provide liberation effectiveness data (stage crushing to determine locked diamond content)

6.12 Ad hoc sampling and assessment of all diamond concentration sections will be conducted to provide baseline liberation data (e.g., XRT feed streams) (stage crushing to determine locked diamond content)

Recovery Efficiency

6.13 Production will be routinely reconciled with the head feed to identify crude anomalies in the expected quality or grade of production. Inquiries into mining, processing, sorting and security processes will be triggered in the event of significant variations.

6.14 Regular tailings audits will be carried out to determine free diamond content and Particle Size Distributions (PSD) are to standard

6.15 Compare In-Situ DSFD's, adjusted for ROM and stockpile sources, with recovered DSFD's, Diamond Footprints and Revenue Distributions to assess overall process recovery efficiency (PRV=Percent Recovered Value) monthly

6.16 Utilise DSFD's and stone counts to check for unexpected changes to recovery frequency of large stones

6.17 Utilise In-Situ DSFD's, Diamond Footprints and Revenue Distributions per source to establish unit process efficiencies

6.18 Production batches will be tracked daily and daily MCF calculated where possible

Design Specifications

6.19 Maintain database of complete conceptual and as-installed process/circuit design specifications

6.20 Maintain database of all equipment design specifications with appropriate as-built drawings and installation standards. Documentation will be current, available and include

- Basis of design, engineering standards and product specifications and other process safety information."
- Context documentation – legislation, codes of practice, and hazard assessment report.

Correct Plant Operation

6.21 Infrastructure, plant and equipment will be maintained, inspected and tested to a schedule that considers design and operating specifications and legislative requirements

6.22 Maintain database of equipment operating specifications/process parameters

6.23 Documentation will be current, available and include Operating criteria - procedures for operation, maintenance and inspections including third-party requirements.

6.24 Maintain database of circuit operating specifications/process parameters

6.25 Document Standard Operating Procedures (SOP's) for all circuits and individual equipment

6.26 Ensure all documentation and databases are kept up to date and changes are managed through the Process Change Database (See 14.4)

6.27 Consider online PSD measuring equipment where practical

6.28 Compile a Standards & Guidelines Document combining all operating standards/measurements to a single, simplified, reference document - specify the standard, measurement frequency and target value or range for all circuits and individual equipment as appropriate

6.29 Compile a Standards & Guidelines Document combining all standards/measurements to a single, simplified, reference document - specify monitoring and control systems used to maintain required target performance

6.30 Compile a Standards & Guidelines Document combining all standards/measurements to a single reference document - specify the best practice standard to aim for if not currently achieved

Plant Information Systems

6.31 Use Management Information Systems (MIS) data historian to capture and archive all pertinent equipment and process data

6.32 Use MIS data to routinely analyse process performance to ensure compliance to standard and highlight deviations for action

6.33 Use MIS data to routinely compile and analyse process mass balances to ensure compliance to standard and feed into continuous improvement programme

6.34 Rigorous use of process change database. All process parameters or equipment changes to be recorded in change database and any change in performance analysed.

Process Simulation

6.35 Plant simulation package to be used to develop a process model (e.g., LIMN, JKSimMet)

6.36 Plant simulation package calibrated against actual performance on a regular basis

6.37 Plant simulation package used to model proposed flowsheet changes before implementation to predict outcomes where possible

Steady State Operations

6.38 Strive for steady state operations in appropriate processes such as, but not limited to, milling, DMS etc

6.39 Strive for steady state operations - minimise the need for operator interventions

6.40 Strive for steady state operations - eliminate spillage

Process Audits

6.41 Process operational audits - regular internal audits of process conformance to standard using comprehensive checklist

6.42 Process audits - annual external audits of process conformance to standard based on minimum performance standards

Cut-off Sizes

6.43 Generate In-Situ Size Frequency Distributions - strive for total content curve but at least finer than expected bottom cut-off size to ensure optimisation of revenue recovery

6.44 Use established in-situ Size Frequency Distributions, Diamond Footprints and Revenue Distributions per source to optimise top cut-off size.

6.45 Use established in-situ Size Frequency Distributions, Diamond Footprints and Revenue Distributions per source to optimise bottom cut-off size.

6.46 Use established in-situ Size Frequency Distributions, Diamond Footprints and Revenue Distributions per source to optimise mid cut-off sizes (re-crush and intermediate large diamond recovery processes)

6.47 Continuously monitor and analyse Size Frequency Distributions, Diamond Footprints and Revenue Distributions as delivered to the plant to determine if changes are required for orebody changes (dynamic Top and Bottom Cut-off optimisation model)

6.48 Formally review cut-off sizes at least annually.

Revenue Loss

6.49 Develop model for calculating revenue loss due to diamond damage

Baseline

6.50 Consider flooring to establish a baseline for fresh breakage.

Damage Evaluation

6.51 Train staff to carry out routine diamond damage evaluations (daily for large stones). (This may only be possible after cleaning at the deep-boil facility)

6.52 Use external subject experts for more detailed breakage evaluations at least annually.

6.53 Analyse diamond damage - Evaluate and track effect on revenue of damage to large stones and ROM production. (Reconstitution method)

6.54 Use DSFD's to check for potential size shifts due to breakage

6.55 Monitor large diamond statistics considering sources mined. Abundance graphs and trends, control charts - large stones per million cts.

Damage Reduction

6.56 Identify areas potentially causing high diamond damage. Assess damage per process, including blasting, and individual units - use diamond simulants.

6.57 Identify areas potentially causing high diamond damage. Assess damage per process, including blasting, and individual units - use low-value diamonds where appropriate.

6.58 Identify and monitor areas of potential impact damage (chutes, stockpiles, individual equipment etc.)

6.59 Reduce diamond damage by applying cost-effective remedial action in high-risk areas according to best practice.

6.60 Monitor changes to diamond breakage after process changes which have potential to increase/reduce damage.

Dilution

6.61 Avoid/reduce dilution in the mining process

6.62 Routinely monitor and record percentage internal waste by source

Stockpile Management

6.63 Operational Procedures will be in place to ensure that, where diamond rich material is stored in a stockyard prior to processing, stockyards/stockpiles will be organised to allow the easy identification of the source of head feed to the diamond liberation and recovery circuits

6.64 The stockyard will be mapped by the geology department and regularly updated to provide an accurate origin of head feed

6.65 Operational procedures will be in in place to prevent waste from being deposited on treatable ROM stockpiles of whatever grade

6.66 ROM will be stockpiled according to grade so separate treatment recipes can be implemented if appropriate

6.67 Operational procedures will be in in place to prevent ore from being deposited on waste dumps

6.68 Operational procedures will be in in place to ensure the stockyard is secured in accordance with the minimum-security requirements in Annex F - Physical Security Controls

Waste Removal

6.69 Technically assess and apply suitable waste removal techniques in the treatment plant. E.g., magnetics removal, preferential crushing techniques

Reconciliation, Accounting and Measurement

6.70 Where the mine site moves its material from the mine site to another place for further sorting before export the second sorting place will reconcile the weights and diamond counts on the same basis.

6.71 At sorting, manufacturing and sales facilities the receipt of goods from the mines is a high-risk activity and will be subject to surveillance review. Goods will be reconciled as soon as practicably possible once removed from the tamper resistant shipping containers.

6.72 When receiving goods from the operations the sales and sorting offices will reconcile the weights and stone counts per size class on the same basis as they were shipped.

6.73 Stock accounting takes place by means of a single electronic accounting system across the diamond pipeline.

6.74 The data will be entered and administered in each accounting system independently and compared by the senior manager in the sort-house at least monthly.

6.75 Production data will be

- Sent daily to the Management Information Systems department.
- Sent monthly to accounting department – this provides a means of comparing data should there be discrepancies.

6.76 Weight reconciliation of production in the recovery plant will be made at the earliest practicable point in the process. This point is likely to be the sort-house or sorting room at the mine site.

MPS 7 - Process Control and Operational Failure Management

Intent

To ensure that operational failures are minimised and the process of mining, liberating, washing, recovering, sorting and selling diamond is clearly understood, in control, measured and reconciled throughout.

Required Actions

Mining

7.1 Mining of kimberlite deposits can expose diamond rich ore, where this is the case care will be taken to coordinate mining and security so that where possible the mining process leaves as little ore exposed as possible.

7.2 Process plants will be established on hard concrete bases with drainage to allow for adequate cleaning away of spillage.

Note: Only buildings such as Crushers, Screens, Water tanks, Bins, Mill, DMS, MDR, Thickener, Recovery, XRT and Audit Plants, this element is compliant.

7.3 For operations and maintenance tasks with significant security risks, identified controls will be incorporated into procedures and work practices.

7.4 The Process Manager and Engineering Manager will determine the optimum mode of operation for control loops in the DMS (or HMS) and Recovery as well as MDR and XRT Plants.

7.4.1 This will be documented and auditable; a record will be kept of any deviation from the optimum mode, who made the change and why (Management of Change process).

Note: The Process change database is used to capture all Engineering and Process changes that are made on the Process Plant and this includes changes that could affect optimum mode. The information includes risk assessment in terms of safety, security and process, why the change, who sensitized the change and whether is a short-term or long-term change.

7.4.2 A list of "bypasses" on the control loops, instrumentation and control circuits will be reviewed for high-risk areas and equipment. These will be repaired with priority.

7.5 The process flow will be used to confirm the results of the following manipulations of process logic are known to operators, security and surveillance.

7.5.1 Altering cyclone pressures.

7.5.2 Altering the density of the Ferrosilicon (FESI) from the norm.

7.5.3 The manipulations, inaccurate and careless installation of DMS concentrate sizing screens and their installation and maintenance.

7.5.4 Turning off the air or water valves to x-ray sorting machines.

7.5.5 Turning off or tampering with the sorters (XRT and Dual Wavelength X-ray sorters) ability to detect and recover diamonds.

7.5.6 The ordinary cycle time of the recovery plant (time from sizing screen to sort-house) will be understood and recorded by surveillance so that they can estimate the time for the above process manipulations to manifest through the plant.

7.6 There are likely to be more manipulations that could adversely affect the security of the product. The Process Manager will list these and ensure appropriate controls are in place to prevent them.

7.7 Power failures/black outs can cause severe degradation of surveillance and other security controls. Where power outages are regular inquiries will be made to see whether they are predictable and so able to be manipulated to assist wrongdoing. If they are then additional controls will be in put in place.

7.8 Operating and maintenance processes and practices will be developed and reviewed in consultation with the people who carry out the work (Briefing records will be filed).

7.9 Task level documentation for operations and maintenance will be accessible and appropriate for the end user.

7.10 This task level documentation will include guidance for surveillance in identifying and managing abnormal situations.

7.11 Documentation for significant risk processes, plant and equipment will be current, available and include Weekly risk reviews (leading) carried out as well as weekly Reports (lagging).

7.12 Basis of design, engineering standards and product specifications and other process safety information.

7.12.1 Context documentation – legislation, codes of practice, and hazard assessment report.

7.12.2 Operating criteria - procedures for operation, maintenance and inspections; and

7.12.3 Third party service/equipment inspection requirements.

7.13 Infrastructure, plant and equipment will be maintained, inspected and tested to a schedule that takes into account; design and operating specifications and legislative requirements.

Behaviours in diamond rich areas

7.14 When in diamond areas the following behaviours will be included in procedures, encouraged and clearly communicated during induction briefs for visitors and training for personnel:

7.14.1 No hand to mouth movements.

7.14.2 Showing of clean hands to camera after handling Diamonds or diamondiferous materials and before leaving the diamond handling area.

7.14.3 Minimise unnecessary handling of product, or product to be handled only as part of a prescribed task/process.

7.14.4 Minimise movement into and out of diamond areas.

7.14.5 Minimise items and possessions taken into and out of gem areas.

7.14.6 No photography without prior written permission.

7.14.7 No hand shaking in diamond areas.

7.14.8 No hand to pocket movement or any other movement that might been seen as “suspicious”; and use of pocketless coats.

7.14.9 Limit the product out of the vault to only goods that are worked on at the time.

7.14.10 No working in the event of exposed product, concentrate or diamondiferous material.

7.15 Surveillance will monitor and report on non-compliance directly to the Security Manager who in turn will report metrics to the Security Control Committee SCC monthly.

7.16 Where required transgressions of procedures and practices will be referred to Human Resources for consequence management.

7.17 A process will be in place to escalate incidents to the Chain of Custody Owners in who's area the incident took place. All incidents will be investigated and learnings from incidents shared with all effected staff.

7.18 Security staff should be well versed and trained to at least a basic level in the production process and understand the diamond winning process. This is to enable them to make informed comment and decisions in the loss prevention process.

Guidance – Reserved

MPS 8 – Maintenance and Housekeeping

Intent

To ensure facilities that concentrate, recover and sort diamonds are kept tidy and subject to an orderly maintenance regime where unplanned maintenance is minimum and managed accordingly.

Note: Frequent and unplanned maintenance in recovery areas can be used to manipulate the process or establish pockets for collecting Diamonds or 'theft lines' like audit lines within the process machinery and piping.

Required Actions

Maintenance

8.1 Planned Maintenance Shutdowns: A procedure will be in place that ensures inspection of any equipment after planned maintenance that occurs in recovery areas. The diamond recovery circuit will not be started until this is done. (The inspection will be done under dual accountability by a plant and security person).

8.2 Unplanned Maintenance: A procedure will be in place that ensures inspection of any equipment after unplanned maintenance that occurs in recovery areas. The diamond recovery circuit will not be started until this is done. (The inspection will be done under dual accountability by a plant and security person).

8.3 Equipment and machinery will be classified according to Security risk and criticality by maintenance (or reliability), security and processing specialists. The asset management strategy will determine the maintenance routine for the various equipment at recovery area:

8.4 Security personnel shall attend maintenance planning meetings and avail resources timely for effective maintenance planning and execution.

Housekeeping

8.5 Demarcation and adhering to demarcation: the storage of equipment and tools will be kept at a minimum in high-risk areas. Areas for storage of equipment will be clearly demarcated and adhered to. There will be no storage of waste products in high security areas.

8.6 Following maintenance or the change-out of equipment, all waste will be removed from high-risk areas within 12 hours. If security is required to clear waste/equipment, the security department will be given prior notice of the maintenance taking place during production and maintenance planning meetings.

8.7 The Security Control Committee members (individually or as a team) will regularly inspect the high-risk areas with a focus on the housekeeping and provide feedback to the Steering committee (ST) meeting at least quarterly.

8.8 Equipment in high-risk areas resulting in spillage will be repaired with a high priority to a state of no spillage. Where regular spillage occurs with no practical solution to repair the equipment, controls will be in place to prevent regular access to the area and the spillage controlled using a hands-off or mechanical method.

Guidance

- It is advisable that a matrix be developed and tracked in SCC meetings as an agenda item.

- Measure planned vs unplanned maintenance – aim to reduce the number of unplanned maintenance events.
- Measure planned maintenance compliance to schedule – aim to match plan and investigate deviation from plan to correct.

MPS 9 - Management of Change

Intent

To ensure that we manage the risks associated with any change to our business processes.

Required Actions

9.1 Change management procedures for any modifications to procedures in diamond areas or where new procedures, equipment, installations, plant modifications, operating models or sites are being assessed for diamond handling activities or within diamond areas will require security's involvement and consultation early in the process.

9.2 The organisation should:

9.2.1 Develop a change control procedure

9.2.2 Obtain management approval and sign-off for the change control procedure

9.2.3 Publish the procedure on the internalised document repository to ensure that it is readily accessible by stakeholders.

9.2.4 Communicate the procedure to employees and relevant external parties

9.2.5 File briefing records

9.2.6 Implement the procedure by establishing a monitoring capability to verify implementation.

9.2.7 Review procedure continually to ensure alignment with business requirements.

9.3 Operations and Security will develop joint procedures in the Recovery, XRT, MDR and Sort-house areas as far as practically possible.

9.4 Operating sites will have a management of change process that governs:

9.4.1 What constitutes a change, and when the change management system needs to be applied.

9.4.2 Requirements for analysing the potential impacts of changes.

9.4.3 Technical knowledge and authority levels required for assessing and approving changes.

9.4.4 How employees affected by the change are involved and the change is communicated.

9.4.5 How information is recorded and updated.

9.4.6 Requirements for post change implementation reviews; and

9.4.7 Contingencies to cover emergency situations where the full process cannot practically be applied.

9.5 All people on site will be trained to identify the change management thresholds specific to their work and how to initiate the process.

9.6 Workplace design and engineering in high-risk diamond areas such as process plants, recovery, XRT, MDR and the sort-house will consider potential security impacts and seek to design security into the operation rather than impose it afterwards once designed.

9.7 Management of change is critical to the upkeep of technical systems. For changes to technical systems, the change process will include a back out plan, backup of initial configuration, stakeholder engagement including a communication plan of the change and updates to the drawings and new configurations.

Guidance

- The early involvement and consultation with security is to ensure that to the greatest extent possible security measures are designed into the operating environment rather than being imposed on it afterwards with the resulting loss of operational efficiency and security effectiveness.

MPS 10 - Sales Controls, Ethics, and Fraud Prevention

Intent

To protect the integrity of diamond sales batches, preserve diamond value, eliminate diamond loss, ensure the longevity for the demand for diamonds and customer retention.

Required Actions

Access control

10.1 All diamond processing operations should be conducted inside an impervious shell and/or a security-controlled perimeter that minimises the risk of unauthorised access to diamonds and/or diamondiferous material.

10.2 Early warning detection systems shall report unauthorised access attempts. Such attempts shall be investigated immediately, and all false alarms eliminated to not create repetitive false alarms.

10.3 All diamond handling areas and associated process units will be protected by means of physical barriers that are implemented pre-emptively through the identified risk profile to prevent unauthorised access.

10.4 Security systems design will be integrated and automated, supporting production where technology used does not compromise security.

10.5 Access control data will be submitted to predictive trend and pattern analysis conducted to determine risk profiles with integrated intelligent systems that automatically flag and drive the risk offensive.

10.6 For each occurrence where diamonds are accessed or processed whether it be diamond batches, diamond parcels, diamond shipments and/or diamond consignments there should be a clear audit trail recording the persons involved, the time duration of involvement as well as the nature of activities that were performed.

Procedures

10.7 All procedures will be:

10.7.1 Current, signed off and comply with the internal requirements, and templates for procedural design.

10.7.2 Readily available for all relevant parties and stakeholders to access.

10.7.3 Communicated to all relevant parties and stakeholders.

10.7.4 Implemented through the establishment of a monitoring process to verify the implementation thereof.

10.7.5 Reviewed continually

Containment of material

10.8 There will be a procedure(s) in place that governs the opening and removal of diamonds from technical sorting equipment following a blockage, stoppage, or anomaly.

10.9 Diamond movement between buildings and facilities should be performed securely, by following the requirements stipulated under MPS19 and controls should be in place to avoid any diamond movement from taking place without security being involved.

Exposure to diamonds

10.10 There will be a procedure(s) in place that governs reporting and rectification of all diamond drops, pick-ups and spillages within the diamond processes. This procedure should also specify the requirements that should be met when detaining people, pending the resolving of weight reconciliation discrepancies to ensure that the human rights of people related to privacy and freedom of movement is not interfered with.

Process auditability

10.11 System information contained in the Stock Management System will be provided in a clear unambiguous format, while Stock Management System reports are to be collated with other security related information.

10.12 Sales operations will:

10.12.1 Establish reconciliation points within the production pipeline

10.12.2 Report all notifications of anomalies via the stock management as well as the Security Incident Management system to management and security staff.

10.12.3 Conduct regular (targeted and random) audits to confirm that physical diamonds are recorded and accounted for by the stock management system.

10.12.4 Provide information for enhanced audit investigations based on reports received from the Stock Management System to analyse information to determine trends.

Weighing and reconciliation

10.13 There will be a procedure(s) in place that governs the way in which weight reconciliation discrepancies or out of tolerances (OTL's) should be handled and escalated.

10.14 All weighing discrepancies that are out of tolerance (OTL) should be escalated in accordance with procedure and recorded by reporting it in the security incident management system.

10.15 An OTL report should be generated to be analysed by an appropriate qualified person or entity independent from the diamond processing operations, at regular intervals as agreed, the results of which should be communicated to a designated audience (Also to be agreed upon) including but not limited to the Risk Manager: Security, who should include this report as part of the overall security metrics.

10.16 An investigation into OTL's should be properly recoded with all evidence recorded for proper management oversight and to enable remote assurance.

10.17 The principle of "two-person accountability" should always be applied during consignment and/or batch weighing and reconciliation to avoid human error.

10.18 Diamond scales will be calibrated by BOBS (The Botswana bureau of standards) at least twice bi-annually and evidence kept for auditing purposes.

10.19 Although essential diamond scale calibrations by BOBS, will not be the only way of verifying scale integrity. BOBS calibrated scales will be counter checked daily by means of "check weighing".

10.20 Each time a diamond weighing discrepancy is detected, as a first order of business, "Check weighing" should be performed to verify scale integrity.

10.21 Diamond batches will always be accompanied by systems generated parcelling letters against which reconciliation will take place.

10.22 Individual diamonds as well as diamond batches will be packed/parcelled and moved/transported in approved containers only.

10.23 Apart from the parcelling letters, container, parcel contents will be identified/described by means of barcoded labels.

10.24 At each reconciliation point within the system, container contents will be verified by:

10.24.1 Scanning the barcodes on the containers with scanners directly connected with the stock management system to circumvent human involvement

10.24.2 Performing positive identification (Verifying that the contents of the containers match the information contained in the parcelling letters and the barcoded labels) of the contents through weigh reconciliation.

10.25 The manual capturing of barcode labels is prohibited and should only be overridden through a change management process, i.e., by submitting and obtaining approval for such deviation by submitting a deviation request.

10.26 Performing unauthorised weight reconciliation off-line is prohibited and should be recorded as an incident (Procedural breach) and immediately escalated for investigation.

10.27 Off-line weight reconciliation may be authorised following a change management process (Deviation request) in the event of diamond weight reconciliation *system failures, at which time additional security controls that are specifically risk based will be assigned. (Refer to systems failure for additional measures).

10.28 As a technical control, diamond weighs should not be captured and/or recorded manually, but rather, scales should be linked directly with the stock management system to enable the automated recording of diamond weights by circumventing human involvement.

10.29 A well-defined procedure involving the principles of “two-person accountability”, consisting of members from security as well as stock control, and the establishment of an audit trail, will be followed for the granting of permission to proceed with diamond processing after a weight reconciliation discrepancy was encountered and the diamond reconciliation system is overridden to proceed.

10.30 All authorised procedural breaches should be reported and recorded in the security incident management system accompanied by the “proof of authorisation” to enable remote assurance.

10.31 The import weight reconciliation report to the government will be systems generated with automated prompting and alert functionality to avoid human error.

10.32 Diamond reconciliation system access will be subject to biometric identification and controlled through the personnel access management system with an audit trail to enable remote assurance.

10.33 Access to the diamond reconciliation system will be removed through a non-human dependant process when no longer required, such as when services are terminated or inter departmental transfers take place.

10.34 Diamond weight reconciliation systems will be designed such that no further diamond processing could take place unless weight reconciliation falls within tolerance and all other criterium is complied with, with an automated alert system via the Fantasy System to notify identified role-players, including, but not limited to security.

10.35 To enable remote assurance, and direct surveillance, non-diamonds and/or gangue found in diamond batches will be:

10.35.1 Checked to verify its non-diamond status following the principle of 2-person accountability, making use of accepted technology, i.e., diamond testers.

10.35.2 Reconciled against overall batch weight

10.35.3 Removed from the diamond batches in a controlled manner, in accordance with procedure.

10.35.4 Handled as if it were diamonds.

10.35.5 Sealed in containers

10.35.6 Dispatched back to the mine in a controlled manner.

10.35.7 Checked at the mine to verify its non-diamond status, making use of accepted technology, i.e., diamond testers.

10.35.8 Discarded at the mine, in a controlled manner.

10.36 The entire process of handling non-diamonds and/or gangue found in diamond batches will be contained in a procedure and recorded in such a way that an audit trail would be available, evidence of which is to be included in the security incident management system.

10.37 Each day, at the end of day, there should be a system generated batch check with automated alarming capabilities to ensure that individual batches are in fact returned for overnight storage.

Diamond damage, breakage and contamination

10.38 The following physical measures should be in place to avoid diamond damage and/or breakage:

10.38.1 Desks for diamond processing will be designed to be “drop friendly”.

10.38.2 Desks should have raised edges that would assist in preventing diamonds from dropping off tables.

10.38.3 Floors in diamond handling area should be carpeted.

10.38.4 Desks for diamond processing should have partitioning in place, (minimum 50 cm high) to avoid accidental batch contamination between diamond sorting stations.

Power supply and systems redundancy

10.39 Diamond processing operations, including security should have a power supply system in place that would be readily available should power supply from the main power grid fail at any time thereby negating a total dependency on the country’s main power grid.

10.40 Based on an analysis of power supply failure durations, the backup power supply should be sufficient to provide uninterrupted operational functionality.

10.41 The backup power supply system will be designed to perform an automated systems check on a weekly basis, that is not human dependent, with alarming capability in the event of a failure.

10.42 Switch-over from the main grid to the backup power supply should be seamless with no apparent interruption in power supply.

10.43 Through a risk assessment process, those critical single points of failure that would result in gross operational disruption and/or immobilisation, should be identified, and contingency plans, including an equipment redundancy plan should be in place to ensure rapid recovery from disaster, as well as uninterrupted systems availability at these critical points.

Systems failure

10.44 There should be a standing operating procedure (SOP) in place that explains the steps that should be followed in the event of a [2]systems failure. Included in the SOP should be the following requirements:

10.44.1 That such systems failure should immediately be reported and recorded.

10.44.2 That diamonds should immediately be separated from human contact.

10.44.3 That, as a first order of business, immediately after systems restoration, weight reconciliation should be performed.

Key management and control

10.45 There will be a procedure(s) in place that governs the management of safe and vault keys.

10.46 All safe and vault keys are to be kept and dispatched from the electronic key management system linked to the access management system making use of the principles of 2-person accountability, such accountability of which should be vested in both the stock control and the security department.

10.47 Information collected in the electronic key management system database will be submitted for analysis with reports included as part of the security metrics.

10.48 The procedure that governs the management of safe and vault keys will stipulate the way in which incidents involving breaches of the key management process should be reported, escalated, and investigated, as an obligatory requirement.

Additional criteria

10.49 To prevent major disruption of operations and/or loss in revenue, there should be a clear understanding encapsulated in written format that stipulates the minimum requirements that diamond shipment, diamond reconciliation, stock control and sales operations should comply with to ensure compliance with:

10.49.1 Insurance requirements to ensure that insurance claims are not rejected.

10.49.2 Government expectations to prevent confiscation of diamond consignments.

10.49.3 Due diligences should be conducted at agreed intervals to verify that insurance requirements and government expectations are:

- Understood and internalised by all stakeholders.
- Complied with as part of the day-to-day operations.
- Included as part of sound governance practices.

[2] *Systems failures include, but is not limited to internet failure, bandwidth limitations, electrical or power supply failure, machine failure, technical failure, equipment failure security control failure or the impeding of systems, equipment and/or machine functionality.

10.50 Security control design, implementation and execution should be void of human based trust relationships.

Process auditability

10.51 Information contained in the Stock Management System should be provided in a clear unambiguous format and be readily available.

10.52 Stock Management System reports should be collated with other security related information.

10.53 Reconciliation points should be established and clearly defined within the production pipeline and regularly reviewed to ensure alignment with business requirements

10.54 All notifications of anomalies via the stock management system should be reported. The reporting platforms should be identified, and the escalation protocols defined in writing, including but not limited to the persons, roles and responsibilities that would be involved in the escalation process.

10.55 Sales operations should have a plan in place to conduct regular (targeted and random) audits in order to:

10.55.1 Confirm that physical diamonds are recorded and accounted for by the stock management system.

10.55.2 Confirm that all non-compliances are reported.

10.55.3 Confirm that non-compliance reports are reduced.

10.56 A written audit investigations process should be in place to analyse information to determine trends based on reports received from the Stock Management System.

Network security

10.57 E-mail correspondence with external parties and stakeholders containing information related to any of the following aspects should be encrypted:

10.57.1 Diamond shipment

10.57.2 Individual diamond and/or diamond parcel descriptions

10.58 The following information security measures should be in place:

10.58.1 BitLocker drive encryption

10.58.2 Perimeter firewall to protect against external/internal threats

10.58.3 Regularly updated antivirus programmes for internal and external threats

10.58.4 Phishing campaigns for user awareness should be performed at regular intervals, the interval durations of which should be clearly defined

10.59 Individual user access to diamond stock control programmes should be controlled by limiting it to only those who need access to perform daily stock control duties and only be relevant for that part, section, or phase that a specific user is required to perform duties at.

10.60 User fields should be defined while multiple user fields per individual, should not be permitted unless specifically authorised after a change management process of which evidence should be readily available, has been followed.

10.61 Individual user access to stock management systems should be gained through biometric login.

Quality control

10.62 There should be pre-identified points within the diamond processing pipeline referred to as quality checkpoints, where [3]quality assurance needs to be performed, the aim of which would be to prevent certain security threats from materialising.

10.63 [4]Quality standards at these "quality checkpoints", should be clearly defined for each point, while those performing quality checks should be trained and declared competent to do so.

10.64 The stock control management system should make provision for the following:

10.64.1 Progress to the next stage or phase within the diamond processing pipeline should not be possible unless quality assurance was performed.

10.64.2 Provision must be made for an audit trail within the system of all quality checks that were performed to enable assurance.

Competent people

The processing of diamonds, and the preparation of such for diamond sales is a specialist function requiring skilled and competent personnel from a variety of disciplines to prepare and secure sales parcels in such a way that diamond value is optimised and events that may be the cause of possible loss of revenue, eliminated.

To achieve this close coordination between the various disciplines is needed, whereby each identified stakeholder within the process knows his/her role and function and are trained and equipped to perform that role and function.

The competency requirement for each role is unique and skills to perform those roles and functions are obtained through a variety of mediums, some being formal and some being informal.

The aim and purpose of the set of criteria that follows will be to establish a system to ensure that persons who have not been equipped for the various roles and functions they perform will not pe

[3] *At certain "checkpoints" within the diamond processing pipeline, especially where human involvement is a primary requirement to process diamonds, capture information and/or evaluate diamonds. At these points a next level of oversight may be needed. These levels of oversight are designed, dependent on the identified need, and may involve peer oversight (Also known as 2-person accountability), such as when weight reconciliation is performed, Security oversight (such as when checks need to be performed to verify that certain procedures were complied with) and supervisory or management oversight (such as when a next level of expertise or authentication may be required).*

[4] *Quality standards are designed to provide clear guidelines to those performing quality checks and may include but need not be limited to setting the minimum sampling requirement.*

permitted to perform those roles and functions unless they have been declared competent, and able to maintain certain competency standards.

Stakeholders/role-players in the processing of diamonds include but are not limited to:

- Stock Controllers
- Diamond Technicians
- Quality Assurers
- Diamond Risk Officers
- Supervisory roles
- Management functions

10.65 The diamond processing pipeline should be clearly defined with most currently updated and signed off PFD's (Process Flow Diagrams) readily available and auditable.

10.66 Roles and functions of persons involved within the diamond processing pipeline should be identified, clearly defined, and linked to the steps, phases and/or stages within that process.

10.67 Competency and skills profiles for each of the roles and functions identified for each of the steps, phases and/or stages within the diamond processing pipeline at the sales offices should be readily available, current, and signed off.

10.68 The way in which skills and/or competencies are obtained should be defined, i.e., formal, or informal.

10.69 There should be a process in place to verify that personnel used in the various roles and functions are competent, having been declared as such and having been certified as such.

10.70 There should be controls in place and where relevant supported by audit trails, to verify that persons will not be used to perform roles and functions for which they are not qualified i.e., for which they have been declared and certified as being competent.

10.71 Where competency requirements involve formal training, authentic records of learning achievements should be readily available for auditing purposes.

10.72 Where competency requirements involve informal, i.e., on-the-job training guidance and/or coaching, such training should be tracked and records maintained (for example a training matrix supported by a training logbook, job observations and assessments etc.) and readily available for auditing purposes.

10.73 As a minimum requirement and in addition to requirements specified elsewhere in the LDCS, Diamond Risk Officers deployed at diamond sales and trading operations should receive training on the following aspects:

10.73.1 Distinguishing between diamond and non-diamond stones.

10.73.2 Knowing the diamond processing pipeline at diamond sales and trading operations and the typical security risks that may be encountered at each of the steps, phases and/or stages including but not limited to knowing how the diamond Stock Management system interlinks with the process and how it functions.

10.73.3 Knowing what their role and function involves when required to perform oversight of processes and transactions including but not limited to the typical errors and/or anomalies that may be encountered that may result in either diamond loss or loss of revenue to .

10.73.4 Understanding diamond evaluation i.e., the 4 C's.

10.73.5 The processes involved when check weighing is performed.

Key equipment and components used in diamond stock control and sales processes processing equipment

10.74 There should be standard in place that specifies the minimum requirements that all key equipment and components used in diamond stock control and sales processes should comply with.

10.75 There should be an equipment redundancy plan in place for all key equipment and components used in diamond stock control and sales processes to ensure ongoing operational

~~MPS 11 – Trading Operations~~

Intent

To provide for additional audit criterium, unique to trading operations, over and above those stipulated under MPS 10 which is also relevant for activities and operations stipulated under MPS11, i.e., diamond trading operations.

Required Actions

Access control

11.1 Records of all access transactions to trading operations should be kept.

11.2 Technical control of people accessing and egressing controlled areas should be auditable, procedural, and integrated with access management system in order to deter and detect unauthorised access.

11.3 Perimeter security and protection measures should be in place based on a risk-based design and aligned to company minimum standards for other parts of the operation(s) (Annex F) should be in place at all places and areas where diamond processing for Trading Operations is performed to prevent potential attempts of unauthorised access.

11.4 Physical barriers, the minimum design specifications of which are risk based should be in place to prevent unauthorised access to diamonds kept and processed at trading operations.

Procedures

11.5 All procedures will be:

11.5.1 Current, signed off and comply with the internal requirements, and templates for procedural design.

11.5.2 Readily available for all relevant parties and stakeholders to access.

11.5.3 Communicated to all relevant parties and stakeholders.

11.5.4 Implemented through the establishment of a monitoring process to verify the implementation thereof.

11.5.5 Reviewed continually

Containment of diamonds

11.6 Material handling systems and processes should be designed to contain product within the diamond pipeline.

11.7 A procedure/s that governs the opening and removal of diamonds from technical sorting (i.e., Sarin machine) equipment following a blockage, stoppage or anomaly should be in place.

11.8 Included in the procedure that governs the opening and removal of diamonds from technical sorting (i.e., Sarin machine) equipment following a blockage, stoppage, should be the requirement that external technicians may not work on or inside machines, unless such machines have been purged first, the implication of which is that they may not physically handle or remove diamonds from machines, and that all machine faults, purging and/or purge overrides should be reported making use of the security incident management system. All SLA's with technical support personnel should accommodate this requirement.

Exposure to diamonds

11.9 There will be a procedure(s) in place that governs reporting and rectification of all diamond drops, pick-ups, and spillages within the diamond processes. This procedure should also specify the requirements that should be met when detaining people, pending the resolving of weight reconciliation discrepancies to ensure that the human rights of people related to privacy and freedom of movement is not interfered with.

11.10 Procedures that govern the way in which diamonds will remain in secure storage, until required for a particular processing activity, thereby avoiding unnecessary exposure will be in place and complied with.

11.11 Included in the procedures that govern the way in which individual stones should be evaluated, should be the requirement that only one stone may be exposed at any given time during the evaluation process.

11.12 Include as part of the golden rules at trading operations the requirement that only one stone may be exposed at any given time during the evaluation process.

Manual handling, processing and information capturing

11.13 Two-person accountability processes, and/or quality control measures involving a next level pf superiority and/or external departmental, i.e., security oversight should be in place as a control measure to avoid human error at pre-identified points within the diamond processing pipeline where the processing of diamonds are primarily conducted through human involvement, included but not limited to the following:

- When repricing the mix-logic.

11.14 When or wherever two-person accountability and/or next level quality control is a requirement within the diamond processing pipeline, the technical system used, i.e., stock control, and/or diamond processing systems, should make provision for a second person to sign in based on his/her authorised user profile within the system and confirm that data arrangements are correct before progress to the next step/phase in the process will be permitted by the system, and an audit trail of the transactions should be readily available, and submitted together with other reports such as OTL reports.

Network security

11.15 All correspondence with outside entities, parties and stakeholders containing information related to individual stones, consignments and/or parcels, including file attachments and adv files, should be encrypted.

11.16 E-mail correspondence with external parties and stakeholders containing information related to any of the following aspects should be encrypted:

11.16.1 Diamond shipment

11.16.2 Individual diamond and/or diamond parcel descriptions

11.17 Individual user access to diamond stock control programmes including but not limited to Fantasy and Galaxy, should be controlled by:

11.17.1 Limiting such access to only those who need access to perform daily stock control duties and only be relevant for that part, section, or phase that a specific user is required to perform duties at.

11.17.2 Making use of biometric login, to gain access to the system.

11.17.3 Defining user fields while multiple user fields per individual, should not be permitted unless specifically authorised after a change management process of which evidence should be readily available, has been followed. The authorisation of multiple user fields to a single individual should only be allowed if the principle if "single person responsibility" is not violated.

Diamond movement

11.18 Diamond movement between buildings and facilities should be performed securely and controls should be in place to avoid any diamond movement from taking place without security being involved.

11.19 There should be a procedure in place that governs the way in which diamonds are moved between buildings and facilities linking the Sales and Clara offices.

11.20 Where diamond processing operations are situated near each other, i.e., when separated by a wall or floor, automated diamond movement, (i.e., vacuum transfer system) should be used as a medium of transport.

11.21 Directly before, and directly after diamond movement, weight reconciliation should be performed an audit trail of which should be available.

Stock control

11.22 The transfer of diamond stock between two different stock management systems (i.e., Fantasy and Galaxy) should be automated, i.e., the systems should be interlinked to ensure a smooth transition of diamond stock between the 2 components and to circumvent human involvement in the transition process.

Diamond damage

11.23 There should be a procedure in place that define the tolerance levels in terms of "chip size" that would constitute a reportable incident in the event of stones that are chipped.

11.24 All incidents involving stone chips exceeding the tolerance levels for "chip size" should be reported to security and recorded making use of the electronic incident management system to enable data analysis and assurance.

People and Culture

MPS 11 - Human Rights and Community

Intent

To obtain and secure a social licence to operate with the communities affected by or surrounding our concessions and demonstrating respect for human rights through subscription to and applying the Voluntary Principles for Security and Human Rights.

Required Actions

12.1 The Company operations will establish a community programme to engage and support the local communities affected by or surrounding our concessions.

12.2 The community programme will establish regular meetings with local communities and the appropriate local authority which will be governed by mutually acceptable charters and recorded as taking place with minutes of the meeting taken.

12.3 There will be a formal and effective grievance procedure that is recognized as such by the local communities' representatives – this will be recorded in the minutes of the meeting.

12.4 Each The Company operation will conduct a human rights and security risk assessment in accordance with the implementation guidance tools of the Voluntary Principles[5]. See Annex H for more information on the Voluntary Principles.

12.5 Where Government Security forces are used in support of the The Company companies will, to the greatest extent possible, include the model clauses recommended by the Voluntary Principles Secretariat in a memorandum of understanding or contract with the appropriate government department[6]. See Appendix 2 of Annex H for such clauses.

12.6 Where there is significant risk of allegations of human rights abuse, The Company will actively seek from the relevant local authorities (e.g., the police, the council, the public prosecutor etc.) information about complaints and do so formally, in writing, at least every two months.

Firearms

12.7 Where public security forces use Firearms, The Company will confirm with them, and where possible have a written protocol in place that requires, that they observe, as a minimum, the UN Principles for the Use of Force and Firearms[7] and particularly seek to use non-lethal weapons in pursuing their duties on The Company concession areas.

12.8 The Company operations will provide training and resources to ensure[8]:

12.8.1 The Company and its personnel will take all reasonable steps to avoid the use of force.

[5] See Implementation Guidance Tools for the Voluntary Principles on Security and Human Rights at: http://www.voluntaryprinciples.org/wp-content/uploads/2013/03/VPs_IGT_Final_13-09-11.pdf other resources are available at: http://www.voluntaryprinciples.org/resources/

[6] See model clauses at: http://www.voluntaryprinciples.org/wp-content/uploads/2016/06/VPI_-_Model_Clauses_for_Security_Agreements.pdf

[7] See the United Nations Basic Principles for the Use of Force and Firearms by Law Enforcement officials at: http://www.ohchr.org/EN/ProfessionalInterest/Pages/UseOfForceAndFirearms.aspx

[8] Based on the requirements of the International Code Of Conduct for Private Security Service Providers: http://icoca.ch/en/the_icoc.

12.8.2 The use of a continuum for the use of force to resolve threats with minimum necessary force.

12.8.3 If force is used, it will be in a manner consistent with applicable law.

12.8.4 In no case will the use of force exceed what is strictly necessary and should be proportionate to the threat and appropriate to the situation.

Guidance:

See Annex H

MPS 12 - Reliable People

Intent

To develop a positive, sustainable Security culture that ensures that people working in at our operations are reliable.

To recruit and retain people of integrity to work on our operations and verify that we do.

To provide the requisite training for our personnel to enable competence and awareness to effectively manage Security risks.

Required Actions

Pre-employment screening and ongoing vetting

13.1 An operation must, in compliance with the applicable laws, verify the identity and credentials of, and undertake checks as to the integrity of, any individual to be appointed to an entrusted role.[9]

13.2 The checks to assure integrity for those recruited to or appointed to entrusted roles will, in compliance with applicable laws, follow the form described in the table below:

Figure 4: The Company vetting matrix

Employment Checks	Purpose: To verify or identify:	Internal Appointments	External Appointments
Identity Check	Candidate identity through government documentation	Required for all roles	Required for all roles
Career History and Employer References	Candidate qualifications Dates of employment, position and reason for leaving previous employers. Match with submitted CV / resume	Required for all entrusted roles where employee has been with The Company Group for less than 5 years.	Required for all diamond entrusted roles
Residential Addresses (5 years)	Match with Career history and identify any inconsistencies	Required for all diamond entrusted roles where employee has been with The Company Group for less than 5 years.	Required for all diamond entrusted roles

[9] An entrusted role will include any role within the The Company operations where there is assigned responsibility over gemstone resources and/or access to or control over business processes which link to the security of the gemstones and there is a risk that fraud or theft on a significant scale could occur.

Employment Checks	Purpose: To verify or identify:	Internal Appointments	External Appointments
Credit Check	Insolvency or credit history that may impact on the candidate's suitability for Diamonds.[10]	Required on initial promotion to a diamond entrusted role and where determined to be necessary, for transfers and promotions	Required for all Diamonds entrusted roles
Criminal Record Check	Criminal records that may impact on the candidate's suitability		
Industrial Psychology assessment[11]	The candidate's propensity for criminality and suitability to work in highly secure areas	Considered for Heads of Department and supervisors in security, recovery and sorting areas	
Polygraph[12]	Assists interviewer detect falsehoods	Required for all roles (Pre-employment vetting)	Required for all roles (Pre-employment vetting)

Inductions

13.3 Induction processes including Security issues will be in place at all operating sites. As a minimum the induction for all employees will cover:

13.3.1 The nature of the diamond business and requirement for more stringent security controls than other businesses.

13.3.2 The operation's security policy.

13.3.3 The security controls they must be aware of in the conduct of their work.

13.3.4 Being subject to surveillance during their work by CCTV.

13.3.5 's responsibility for personnel security.

13.3.6 The importance of following operational procedures and letting their supervisors and leaders know if they do not understand the procedures or the procedures are unclear.

13.3.7 Their obligation to report wrongdoing or suspected wrongdoing.

[10] Where legally acceptable (i.e. it is not legal in Mozambique for non-financial institutions to do this).

[11] Where the General Manager approves the cost for supervisory roles in higher risk gemstone handling areas or the security team.

[12] Where legally applicable.

Training

13.4 There will be a process for delivery and maintenance of competency-based training for the Security Team and personnel working in high-risk diamond areas that includes and integrates the practical management of Security risks.

13.5 All personnel working in diamond areas [including Security personnel] or in diamond entrusted roles will undergo specific training related to Security in the conduct of their duties.

13.6 Where there is a requirement for interventions into the diamond recovery circuit, and it is practicable to do so, a standard and authorised method of doing the task should be developed with an associated Single Point Brief and these should form part of the security awareness training.

13.7 Security awareness training delivered to those people working in high-risk diamond areas is to focus on the specific requirements and expectations of the outcomes of the security or diamond controls rules and procedures.

Standard Operating Procedures and Golden Rules

13.8 All departments should produce Standard Operating Procedures (SOPs) detailing the steps to take for all tasks.

13.9 The SOPs for higher security risk diamond areas will be particularly detailed and inform surveillance in identifying non-conformities.

13.10 The SOPs for higher security risk diamond areas should be distilled into Single Point Briefs making use of pictures and simple instructions which will be posted where the task takes place and used to inform training (and surveillance observations).

13.11 The operation is encouraged to develop a short list (should not be more than 7 key points) of Golden Rules which all personnel will be made aware of and must follow, and which carry consequences if they are not follow.

Consequence Models

13.12 The Human Resources team will develop a clearly understood consequence model for breaches of Golden Rules. This will be explained to all personnel. [Guidance: where possible personnel should sign the Golden Rules to confirm that they fully understand them and the implications of not observing them.

Exit Process

13.13 The Human Resources team will inform the security team within one day of any personnel that have resigned and are serving out their notice.

13.14 All employees that have worked in diamond areas will be asked for their impressions of security as part of an exit process[13] on leaving an operation or The Company.

13.15 People leaving employment within Diamond areas or The Company operations will be reminded in writing of their obligations of confidentiality before they leave.

Guidance – Reserved

[13] By a manager once removed, a security manager or someone from Human Resources.

MPS 13 - Engagement and Communication

Intent

To communicate effectively with our stakeholders and engage all personnel in contributing to our success. Security and Security Controlis not a security only responsibility but should include all staff.

Required Actions

14.1 There will be an effective two-way Security communications processes put in place to support this. The Security Manager and Security Team will continuously engage the entire workforce in the security program and there have an ongoing employee engagement plan in place. The intention is to create a security community at the workplace that consist of all.

14.2 All employees should have a basic understanding of the security risks in the workplace and how to deal with them to ensure that assets are protected. This should be included in the employee induction program and cover topics like, the crime continuum, nature of theft and reasons why people steal and countermeasures to prevent theft and loss. Most people are honest and this should be the focus of the training so that the majority will see the value in the protection of from losses.

14.3 All employees should know how to report security incidents and/or security failures. Such reports should be investigated with feedback to the reporter. The number of such reports should be tracked and reported to the SCC on a quarterly basis. Effective plans should be put in place to encourage reporting by employees.

14.4 An employee engagement survey should be conducted at least every second year to measure the extent of employee involvement in the security program and well as their view of the security effort. Feedback should eb provided and their assistance sought to improve security engagement.

14.5 All leaders / Heads of Department / Chain of Custody Owners at the operation will be able to answer these questions:

14.5.1 Do we have a list of all our assets and know where they are?

14.5.2 What are the specific risks in this area that could contribute to the loss of product and assets?

14.5.3 How are these risks controlled?

14.5.4 What is your specific role in ensuring that these controls are in place?

14.5.5 What will you do if you see that one of these controls is not in place?

14.5.6 How do you work with Security to continuously improve security of assets?

14.5.7 Consultative processes will be in place to identify, assess and control security risks at operational, task and individual levels.

14.6 The security department will assist Leaders / Heads of Department / Chain of Custody Owners to put security plans in place for the areas under their control and ensure that those plans are executed by the security team members.

14.7 The Risk Manager: Security will brief all new managers and Heads of Department on our approach to their specific accountability within two weeks of their arrival in post. This briefing will be recorded in the minutes of the next Security Control Committee meeting.

14.8 Each operation will determine working languages in diamond areas so that work can be conducted safely, and communications understood by management, workers and security. [Guidance: where groups of people are working the language will be understood by all group members or there will not be side discussions in a language that others do not understand.

Signage

14.9 Each operation should develop signage supporting security communications. Such signage could:

14.9.1 be posted prominently at the entrance to diamond areas, and mine site entrances.

14.9.2 make use of simple pictures to explain their points.

14.9.3 be in English and the local language; and

14.9.4 indicate that cameras are used for surveillance.

Guidance

- External stakeholder engagement is also key.
    - They include law enforcement agencies and diamond security organisations.
- A strong relationship and a good working environment conducive to co-operation is needed if the malicious and non-malicious loss of precious stones is to be stopped at our mines and across into other countries.
- So, collaboration between law enforcement agencies and diamond security must be nurtured.

MPS 14 – Continuous Improvement

Intent

To ensure we continuously improve our approach to Security with knowledge gained from incidents, non-conformities, new operations, questioning from stakeholders and management review of this Standard.

Required Actions

Security Incident Reviews

15.1 Each site should have a system and procedure for managing Security incidents that specifies requirements for: reporting, recording, investigating, analysis, managing actions and communications.

15.2 An incident escalation procedure should be developed and followed.

15.3 All incidents, including near hits, should be reported.

15.4 All incidents will be classified and reported based on maximum reasonable outcome (MRO) and actual outcome using the The Company 5x5 risk matrix – See Annex C.

15.5 All recordable losses, significant incidents (including significant potential incidents), will be reported to the General Manager (as soon as possible) and to the MD of The Company (within 24 hours).

15.6 External reporting of incidents to regulators will occur in accordance with relevant legislation and be managed by the operating site with advice from legal counsel.

15.7 For each incident, an accountable leader will be responsible for ensuring a timely investigation appropriate to the risk and complexity. The Managing Director of The Company or the The Company Diamond Corporation Chief Executive Officer will mandate and delegate the appropriate level and type of investigation that is required.

15.8 Investigations will be supported by competent people, appropriate to the risk and complexity of the circumstances. Decisions on who supports investigations will be authorised by the General Manager.

15.9 There will be a process for recording, approving and implementing business improvement recommendations arising from incident investigations.

15.10 There will be a process for reviewing the status and effectiveness of implemented controls for significant Security incidents over time.

15.11 Learnings from significant Security incidents will be shared across the The Company business within seven days. An example of such a communication is at Annex M.

Guidance – Reserved

Protection

MPS 15 - Physical Security

Intent

To ensure that we have adequate physical security measures in place that are integrated with people, procedures and technical systems.

Required Actions

Security Policy

16.1 A security policy must be in place. By in place, it is implied that the policy is:

16.1.1 Published on the internalised document repository and readily accessible to all stakeholders.

16.1.2 Communicated to employees and relevant external parties.

16.1.3 Monitored to ensure its continuous application.

16.1.4 Reviewed as and when circumstances may dictate but at least once per year to ensure alignment with business requirements.

16.2 Evidence that input was received from stakeholders and accommodated in the policy must be available.

16.3 Procedures that support the policy must be in place, by in place it is implied that the procedure is:

16.3.1 Aligned with the physical security policy.

16.3.2 Implemented based on management approval and sign-off.

16.3.3 Published on the internalised document repository and readily accessible by all stakeholders.

16.3.4 Communicated to employees and relevant external parties.

16.3.5 Monitored to verify its continuous application.

16.3.6 Reviewed as and when circumstances may dictate but at least once per year to ensure alignment with business requirements.

Design based on reliable risk assessment.

16.4 The physical security design will be based on a risk assessment that exhibits a clear understanding of:

16.4.1 The The Company facility’s operations and conditions.

16.4.2 Threats to the organisation reflected in a threat register based on a threat analysis that highlights priority threats.

16.4.3 Vulnerability severity based on a vulnerability assessment of the various lifecycles, processes and facilities in the organisation.

16.4.4 Prioritised risk levels reflected in a risk register that is dynamically updated to reflect real security risk to the organisation.

16.4.5 Risk mitigation, whereby:

16.4.5.1 An action plan is compiled to mitigate the identified risk.

16.4.5.2 The action plan is executed, monitored and controlled.

16.4.5.3 Management is provided with feedback showing the level of risk mitigation achieved.

16.4.5.4 The security control environment where controls are measured and monitored on a continuous basis to reflect control relevance, effectiveness and to verify that real risk is in fact mitigated.

16.5 Risk awareness is reflected within the various levels of the organisation, including but not limited to:

16.5.1 Senior management level i.e., baseline risk register reflecting the organisation security risk profile.

16.5.2 Issue based level, i.e., supported by a mechanism whereby day-to-day risks are identified, analysed and incorporated into the organisation risk profile so as to keep the risk profile current and up to date.

16.5.3 Supervisory level i.e., risk identification, mitigation and control verification for each job or task, whether formal or informal.

16.5.4 Employee level, i.e., continuous risk management by each employee within the organisation.

16.6 A mechanism to identify and mitigate critical risks supported by a TARP, Trigger Action Response Plan, or any similar mechanism is in place to ensure resilience, i.e., recovery from disaster within the shortest period.

16.7 Critical risk identification should reflect the common mode failure points where the failure of a single element of the security system significantly compromises security.

16.8 Risk management and risk assessment practices are integrated in project management system verified by the fact that information collected during the risk assessment phase, including risk mitigating measures is recorded and stored with the engineering documentation.

16.9 Risk mitigation implementation is well supported by a quality assurance process whereby any new installation for a technical device (Sensor, Camera etc.) will have a technical evaluation completed, while non-technical installations undergo scrutiny to verify the quality of the installation in support of the risk assessment and to verify that the intended benefit has been realised.

16.10 The physical security controls outlined in Annex F will be expected, unless a risk assessment determines otherwise, in which case Annex F will be reviewed to reflect the findings of the risk assessment i.e., Annex F forms part of the mandatory requirement.

Perimeter Protection and Access Control

16.11 Diamond facilities will have perimeter protection measures in place as outlined in Annex F, to protect the product and personnel and allow for the imposition of access control. Fence design should be based on a risk assessment identifying the clear and present threats and vulnerabilities, taking into account the way in which the threats may exploit the vulnerabilities. Fence design must be such that it mitigates the risks that have been identified during the risk assessment.

Example 1 – In Northern Canada the erecting of fences is impossible due to the snowfall that makes fence maintenance impossible and impractical. The operation there have implemented video covered surveillance “fencing” that alerts access. It should also be noted that the closest communities are hundreds of miles away that makes access the sites in summer almost impossible and in winter only by winter roads that are well patrolled.

Example 2 – The diamond vessel operating at sea does not have a fence around it for obvious reasons but means of access to the vessel is monitored by intrusion systems and cameras creating a virtual fence.

16.12 The organisation must:

16.12.1 Develop an access control procedure or procedures that govern the authorisation of required access into various areas.

16.12.2 Communicate the procedure that governs the authorisation of required access into various areas to relevant external stakeholders.

16.12.3 Implement the procedure that govern the authorisation of required access into various areas by establishing a monitoring capability to verify implementation.

16.12.4 Review procedure that governs the authorisation of required access into various areas as and when circumstances may dictate but at least once per year to ensure alignment with business requirements.

16.13 As a minimum requirement the access control procedure must contain the requirement that, the mine, process plants, recovery areas, sort-houses and other diamond areas will control access and record the movements of all personnel, vehicle and material movement in and out of the area. The level of access is determined by the risk profile of the area and should be reflected in the procedure as such.

16.14 Access and egress patterns for all people, vehicles and goods/materials must be auditable and data readily available on an electronic platform for analytical purposes.

16.15 Reasons for access into high-risk areas, processes and machines and the man-hours spent in proximity and/or contact with diamondiferous material must be recorded for statistical purposes to manage and reduce physical contact with diamondiferous material.

16.16 Reasons for access into high-risk areas will be based on a specific need to access and approved by the Risk Manager (Security).

CCTV Coverage

16.17 Visual chain of custody of interactions between product and people is required. The layout of CCTV cameras will be finalised after the process and security stakeholders agree to the camera purpose and expected outcomes.

16.18 Camera placement and application will be fit for purpose, based on a camera risk assessment that considers but is not limited to:

16.18.1 Camera functional requirement

16.18.2 Camera technical specifications

16.18.3 Recording requirements

16.18.4 Redundancy requirements

16.19 A fixed camera footprint will be used for diamond areas and PTZ will only be used as secondary support. In any high-risk diamond areas, cameras will cover all locations where there is people and product interaction and the flow of people and product through the area.

16.20 Standby, portable cameras should be readily available inside high-risk areas to mitigate security risk in accordance with a Job Risk Assessment, that is conducted prior to all high-risk area equipment/human interfaces, should the fixed camera footprint proof inadequate to mitigate the identified risk.

Biometric scanners

16.21 At dedicated entry points of the mine and all diamond handling buildings, biometrics will be used as an identification tool.

Security Zoning

16.22 Security zoning at Karowe Mine and Corporate Office (Diamond Technology Park) shall conform to the following:

16.22.1 White Area - Zone One:

The white area zone consists of:

16.22.1.1 public access areas.

16.22.1.2 Outside Mine perimeter and at public foyers

16.22.1.3 Areas with limited security controls.

16.22.1.4 Security measures should include perimeter access control.

16.22.2 Green Area - Zone Two:

The green zone consists of

16.22.2.1 The area surrounding the mine facility or site up to the outer perimeter of the Blue Area. Restricted Access is allowed to:

- Employees
- Visitors (Only with prior arrangement)
- Suppliers (Only if delivery is validated)
- Contractors (Only if officially contracted)

16.22.2.2 Security measures should include perimeter access control and security clearances of those entering.

16.22.3 Blue Area - Zone Three:

Blue areas are classified based on a risk assessment and include but need not be limited to:

16.22.3.1 the enclosed security area incorporating the opencast pit, underground mine entrances, workshops, offices, milling, crushing, feedprep, and DMS sections of the Treatment Plant.

16.22.3.2 Security areas within company premises with additional access controls on staff.

16.22.3.3 Areas for valuable assets with specific item asset protection controls and tightly controlled public access. (Include Pit and Process Plants).

Limited employee and contractor access is allowed, and visitors should be escorted or tightly controlled.

16.22.4 Red Area - Zone Four:

16.22.4.1 Red areas are classified based on a risk assessment and include but need not be limited to:

16.22.4.2 The area where the product is found in concentrated form such as the Red Area DMS (cyclone spigot and sink screens), Concentrate Bins, Tomra Machines, Recovery Plant, auxiliary equipment, (XRT & MDR), Sorthouse, Cleaning Facilities, Sales and Marketing diamond processing areas.

16.22.4.3 highest security areas in company premises and Production high-risk areas.

Employee access will be strictly controlled based on a need to enter, through personal identity verification, i.e., biometrics, as well as card access. Only contractors and visitors with a need to know and closely escorted will be authorised to enter.

16.23 The red or high-risk area in a mining concession must comply with the following as minimum requirement:

16.23.1 The red or high-risk area must be situated inside an impervious shell and/or have perimeter security that will minimise the risk of unauthorised access and theft of diamonds and/or diamondiferous material.

16.23.2 All process streams and associated process units will be protected by means of physical barriers to prevent unauthorised access.

16.23.3 Access to process control units must be controlled through the electronic access management system. and if this is not possible, access to be controlled by means of an electronic seal management system in conjunction with intelligent padlocks and or numbered seals.

16.23.4 Provide for audit trails whereby access to process units and the reasons for gaining access can be monitored.

16.23.5 Where physical contact is possible between members of the blue and red areas, the red or high-risk area must have a double perimeter protection facility with a no-man's land in-between to reduce contact with people not situated in the red area.

16.24 Prioritising of alarms (and their annunciation in the alarm monitoring system) should follow from these layers with the alarms on the most likely targets given clear priority over other alarms or notifications.

16.25 The surveillance room and security data equipment room will be within a wider security perimeter and have additional access control specific to the people that need to work there and have visual signs indicating that only authorised personnel may enter.

Key Control and Padlocks

16.26 The use and distribution of keys and padlocks will be tightly controlled and subject to written protocols. The protocols will ensure these controls are in place and describe the methodology supporting dual-key systems, and any variances.

16.27 Padlocks are not to be left unlocked and unattended. When padlocks are not securing the item, - (for instance if maintenance is being carried out) they should be locked and secured to another place so that they cannot be swapped.

16.28 Access to keys should be controlled in a manner that is auditable and based on confirmed personal custody of keys. [Guidance: This is likely to be achieved through the use of either biometrics or access control cards to access the key cupboard.]

16.29 The Risk Manager: Security will ensure a random audit of key control at least every quarter and report findings to the operation's SCC.

[Guidance – Key Control and Padlocks: Where operations personnel control one of the dual custody keys the chain of custody owner is responsible for the security of the key and should be made aware of the importance of key control by the Security manager.]

Seals

16.30 The placement of a seal will not be considered as providing a physical security control on its own.

16.31 The selection of seals will be based on the security requirement according to risk. Seals that protect high value goods will be uniquely numbered, not readily copied or reproduced and their continuity proven when used.

16.32 The Risk Manager (Security) will arrange for regular, random audits of high-risk seals and report on these to the SCC. The following must be verified during seal audits:

16.32.1 Unplaced seals are safely stored and dispatched from a single point of control. All dispatches are accounted for.

16.32.2 Seal batches are issued to only a limited number of persons who have been clearly authorised to be in possession of such seal batches. Seal batches are kept/stored safely.

16.32.3 A clear and auditable record of seal batches that were issued are kept and all seals are accounted for.

16.32.4 A clear and auditable record of seal issued and deployed at machine and component interfaces is kept.

16.32.5 Seals applications are verifiable and correspond with records.

16.32.6 A clear and auditable record of seal removals are kept with reasons for such clearly reflected. All removed seals are accounted for.

16.32.7 Seals are declared redundant and discarded only after verification and sign-off by the seal management chain of custody owner, and only if he validity of the seal lifecycle could be verified.

Searches

16.33 All personnel, personal possessions, items, equipment and vehicles entering or leaving high-risk Diamond areas will be subject to search and procedures will exist detailing the search techniques.

16.34 Movement of personnel, goods, equipment and vehicles into and out of the high-risk diamond area will be recorded electronically with a clear audit trail.

16.35 The organisation should:

16.35.1 Develop a procedure that governs the processes that must be followed in order to get authorisation for the removal of assets from the operation and the return thereof.

16.35.2 Obtain management approval and sign-off for the procedure that governs the processes that must be followed in order to get authorisation for the removal of assets.

16.35.3 Publish the procedure that governs the processes that must be followed in order to get authorisation for the removal of assets on the internalised document repository.

16.35.4 Communicate the procedure that governs the processes that must be followed in order to get authorisation for the removal of assets to employees and relevant external parties.

16.35.5 Implement the procedure that governs the processes that must be followed in order to get authorisation for the removal of assets by establishing a monitoring capability to verify implementation.

16.35.6 Review the procedure that governs the processes that must be followed in order to get authorisation for the removal of assets continually to ensure alignment with business requirements.

16.36 The organisation should:

16.36.1 Develop a procedure that governs the quality of repairs.

16.36.2 Obtain management approval and sign-off for the procedure that governs the quality of repairs.

16.36.3 Publish the procedure that governs the quality of repairs on the internalised document repository.

16.36.4 Communicate the procedure that governs the quality of repairs to employees and relevant external parties.

16.36.5 Implement the procedure that governs the quality of repairs by establishing a monitoring capability to verify implementation.

16.36.6 Review procedure that governs the quality of repairs continually to ensure alignment with business requirements.

16.37 The organisation should:

16.37.1 Develop a procedure that governs the processes that must be followed when disposing of redundant assets, including the manner in which secure data must be handled.

16.37.2 Obtain management approval and sign-off for the procedure that governs the processes that must be followed when disposing of redundant assets.

16.37.3 Publish the procedure that governs the processes that must be followed when disposing of redundant assets on the internalised document repository.

16.37.4 Communicate the procedure that governs the processes that must be followed when disposing of redundant assets to employees and relevant external parties.

16.37.5 Implement the procedure that governs the processes that must be followed when disposing of redundant assets by establishing a monitoring capability to verify implementation.

16.37.6 Review the procedure that governs the processes that must be followed when disposing of redundant assets as and when circumstances may dictate but at least once per year to ensure alignment with business requirements.

16.38 All security personnel will be trained in the conduct of thorough searches of personnel and equipment. This training will be refreshed at least every six months and an auditable record of such training should be maintained.

Personnel Searches

16.39 People entering the diamond area will be made aware of the requirement to submit to a search before they enter the diamond areas as part of the diamond areas briefing. They will give their written consent to undergo searching before entering the diamond areas.

16.40 Signed records of permission to be searched obtained for employees, contractors, suppliers and visitors must be kept and readily available for audit and investigation purpose.

16.41 A waiting area will be made available for people to be held immediately preceding the exit process and so possibly about to undergo the search. The waiting area will be subject to surveillance.

16.42 The area that people wait in before the exit and search process will be equipped with devices for the person to clean themselves of any diamond product or diamond resembling material. This equipment will as a minimum include strong wire brushes for cleaning the soles and welts of shoes and boots; a device for picking stones from shoes; mirrors; and an honesty or “last chance” box for any diamond material found.

16.43 The methodical search will comply with a written search procedure and a Single Point Brief that will be prominently displayed to those about to undergo the search process and in the search area itself.

16.44 The procedure will detail the response that will be taken if; unusual behaviour is observed, or something of interest is found and stipulate the chain of custody and preservation of evidence protocols to ensure there is no tampering with the items of interest.

16.45 All entries and exits to the high-risk diamond areas will be recorded so that subsequent analysis can be made of ratios of people searched.

16.46 Searches will be conducted and witnessed by people of the same sex as the person being searched.

16.47 Searches will be witnessed (surveillance can provide a witness if appropriate) and the following will be recorded:

16.47.1 time of the search,

16.47.2 name of the person being searched,

16.47.3 name of the person doing the search and

16.47.4 name of the witness, as well as

16.47.5 the level of the search.

16.48 Where there is a reliance on physical searches of the person there will be at least two levels of personnel search:

16.48.1 A Physical full body contact search that checks the bottom of the boots and another place chosen at random such as the inside of the mouth, the belt line or the person's hair; and

16.48.2 A Full strip or rigorous searches down to underwear in all high-risk areas and, as and when circumstances may dictate.

16.49 Where x-ray searching of personnel is conducted, records of x-ray searching data in compliance with legal requirements at the country of operation must be kept and readily available for interrogation/audit purposes and analysis.

16.50 X-ray scanning data must be kept at an off-site facility, from where data analytics is possible free from interference of on-site personnel.

16.51 Data must be current and secured through regular back-ups in an off-site facility.

16.52 Personnel x-ray equipment is managed within clearly defined operating parameters.

16.53 Personnel x-ray data protection should be codified and clearly defined through a written protocol.

16.54 All escape routes shall be designed to conform to the local regulations applicable to emergency exits. The emergency exit doors will release in a manner that persons will be routed to safety in a direction away from the danger area without compromising the high-risk area security.

16.54.1 Exit from the high-risk area will as far as possible be into a safe refuge bay, fully equipped to:

16.54.1.1 Accommodate personnel during an emergency. The emergency exit procedure shall be fully auditable. All emergency exits will be alarmed by the Access Control System and monitored.

16.54.1.2 Provide a means of CCTV surveillance.

Guidance – Personnel Searches

- *Decisions on who should be searched and to what level should be risk based. Where someone has done something that warrants investigation, they will undergo a rigorous search. Similarly, the chain of custody owner in consultation with the Risk Manager (Security) can mandate increased or decreased levels of full search.*

- *This technique provides an opportunity to interact directly with the person in the search room. This time should be used to assess the reaction of the facial and body language of the person being searched. On occasion the time might be used to interview a person rather than searching them before they are released from the diamond areas. Any such interactions should result in a report held in the security incident management system.*

- *Consideration should be given to the use of technology to assist in personnel and equipment searches. Such technology could include millimetre wave and x-ray scanners.*

Searches of Equipment and Rubbish

16.55 Freight handling facilities must be in compliance with the requirements stipulated in Annex F, Freight handling procedures must be approved, implemented and regularly reviewed.

16.56 Red Area Freight Facility (Single Airlock system):

16.56.1 All red area freight handling activities to and from the Recovery (XRT and MDR), Sorthouse and DMS concentrate areas shall be via the Red Area single airlock freight facility.

16.56.2 The airlock shall form part of the impervious shell and shall be equipped with access-controlled roller shutter doors.

16.56.3 Roller shutter doors shall be equipped with electric motors to facilitate remote operation of the doors.

16.57 All equipment and personal effects brought into and taken from diamond areas will be subject to searches.

16.58 The accountable manager of the diamond areas will approve in writing, all non-standard equipment (one off introduction of, or project related equipment) taken into and out of the diamond areas before it is brought in or taken out.

16.59 A written protocol should dictate the manner in which redundant equipment should be treated and also specify at what stage equipment will be considered redundant, in which case the use of it should be prohibited and the removal of such facilitated.

16.60 Decisions on what is searched and to what level will be risk based and recorded in the security incident management system.

16.61 Where standard tools are frequently required by mechanics, engineers or electricians, consideration should be given to holding a set within the diamond areas that does not leave this area.

16.62 All rubbish and waste from diamond areas will be searched and the search witnessed (surveillance can act as a witness to this).

16.63 The waste will be disposed of such that it is not easily identified as coming from the diamond areas and not easily recovered.

16.64 Liquid and toilet waste outlets and drainage systems and access to them will be monitored.

Guidance – Searches of Equipment and Rubbish

- *The number of items taken into diamond areas should be minimised and clearly thought through:*
  - *Where an item of equipment is needed, consideration should be given to removing its packaging before entering the diamond areas; and*
  - *Where appropriate items taken into diamond areas will be searched to mitigate the risk of substitution.*
- *The search equipment might include mirrors on poles, x-ray machines, dentist mirrors, or other specialist devises as required.*

MPS 16 – Technical Systems

Intent

To ensure that the technical systems on which our security relies are fit for purpose, well maintained, resilient and proactively managed to optimise their performance.

Required Actions

Controls

17.1 In high-risk areas, controls will be selected and placed only after the purpose and expected outcomes have been defined and approved as part of the risk assessment process.

17.2 The technical security controls detailed in Annex G – will be expected to be in place unless a risk assessment determines otherwise – i.e. Annex G forms part of the mandatory requirement.

17.3 All security electronic controls will be monitored on live basis to ensure the security equipment live status and ability to perform its desired function. The surveillance team will monitor the security equipment. These devices include.

17.3.1 Cameras

17.3.2 CCTV Servers

17.3.3 Network Switches

17.3.4 UPS Equipment

17.3.5 Future access control and alarm equipment

17.4 Security control equipment and security panels will be fitted with tamper switches and configured to annunciate to the surveillance team any system tampering or unavailability of equipment.

Security System Access

17.5 The Company users of the security network and systems will be held accountable for their actions. All security systems will have unique individual logins to access software. This will include security contractors as well.

17.6 Passwords will comply with The Company IT Security Policy.

17.7 Admin accounts will not be used unless required by technical staff for specific changes. The users of the security systems will be audited as part of the regular technical maintenance.

Power

17.8 In the event of a power failure all security systems in the Red Areas (See MPS X for Red Area Definition) will stay on either through connection to a UPS and or Generator. These systems and back-up power shall be configured in such a way that no security capability is lost.

17.8.1 A power failure will be simulated at least once per month to ensure these power back-up systems kick over seamlessly and all staff are familiar with operations in the event of such failure.

17.9 In the event that the power failure will last for periods longer than that of the power back-up measure the systems should be shut down in a controlled way and the areas evacuated until power is restored. The Security systems in these areas should be seen as an integral part of the production systems and the one cannot operate without the other.

17.10 All The Company security systems are to have spike and surge electrical protection installed. Security equipment specifications should include surge protection.

17.11 Continuity of power supply will be provided for all technical security systems as per 17.8 above . As a minimum, UPS battery uptime will be 30 minutes when a generator is provided. Where a generator is not provided, UPS uptime must not be less than 60 minutes to complete an automated shutdown of downstream equipment and evacuation of high risk area as per 17.9 above.

Environmental Conditions

17.12 Computing and electronic equipment that contributes to the security system will be kept within the environmental parameters recommended by the manufacturer.

17.13 All decisions surrounding the maintenance, design and removal of air-conditioning, power, and lighting infrastructure will engage the Engineering Manager his/her delegate and the Risk Manager – Security.

Technical Support

17.14 A preventative maintenance plan will be in place to test and ensure the correct operation of the controls at regular intervals. This maintenance will be documented and reviewed monthly. See the Appendices of Annex G for copies of the individual maintenance plan and yearly calendar.

17.15 Technical systems will have a dedicated resource to oversee the support of these systems. The position will report directly to the Risk Manager – Security.

17.16 The Risk Manager – Security will put plans in place to ensure that the Technical Security function and capability is continuously audited for compliance and possible manipulation of systems as the security systems are key to protection at source.

17.17 A dedicated fault reporting mechanism will be in place that allows staff to report faults. This mechanism will have the ability to:

17.17.1 Report the asset failed and provide supporting information.

17.17.2 Allow the technician to log the reasons for failure and how the repair was completed.

17.17.3 Communicate the status of the repair.

17.17.4 Allow the interrogation of an asset to see fault history.

17.17.5 Critical Systems availability will be tracked and reported to the SCC on a quarterly basis. At minimum this should include:

17.17.5.1 Camera Availability by Red Area and Blue Area respectively

17.17.5.2 Personnel Search systems like x-ray machines

17.17.5.3 Access Control Systems in Red and Blue Areas respectively

17.17.5.4 First, Second Tier and Remote Security Surveillance/Assurance Systems

Disaster Recovery for Security Systems

17.18 All high-risk security equipment will have a disaster recovery plan to minimise the downtime of unexpected events and reduce the impact on security operations.

17.19 The following Backups of security systems and equipment must occur:

17.19.1 All Servers ("snapshot" backups) with a back up to be held off site.

17.19.2 All network equipment (configuration backups).

17.19.3 All Security Panels (configuration backups).

17.19.4 All other electronic devices (configuration backups).

17.20 Procedures and quick check sheets for disaster recovery will be available for technical staff to refer to and decrease outage times.

17.21 A comprehensive and accurate inventory is maintained containing:

17.21.1 Systems information

17.21.2 Systems vulnerabilities

17.21.3 Causes of failures

17.21.4 Downtime

17.21.5 System replacement and maintenance protocols

17.22 Policies and procedures that governs the way the inventory systems are compiled, maintained, used, managed and controlled, including patching and the associated roles and responsibilities is in place and readily available.

17.23 Network (security) architecture diagrams, strategies, policies and procedures are available, demonstrating the organisation's approach to defining and implementing distinct network security domains or zones (e.g., WAN-DMZ-LAN, CCTV and card access networks).

17.24 The network/systems architecture provides for the synchronisation and coordination of various system timekeeping components, including but not limited to surveillance equipment, access control equipment networking devices and the incident management system.

17.25 Available evidence suggests that the organisation has designed, implemented, checked, used, managed and maintained:

17.25.1 Suitable malware controls

17.25.2 Policies, procedures and guidelines

17.25.3 Architectures/designs

17.25.4 Contracts

17.25.5 Records such as details of malware incidents, antivirus program and signature file update histories.

17.26 IT development, test, production and support environments are distinguished, kept separate and controlled, including how they are migrated, checked in/out or promoted between them.

Network and server capacity and performance management

17.27 Installation and configuration of IT systems:

17.27.1 Backups and archives

17.27.2 Job scheduling

17.27.3 Errors, alarms and alerts, plus logging and monitoring

17.27.4 Patching

17.27.5 Change management and version control.

17.28 Clear-desk clear-screen policies and procedures are readily available and implemented.

17.28.1 Compliance to clear-desk and clear-screen policies is assessed by means of security personnel conducting workplace inspections during or outside normal working hours.

17.28.2 Incidents related to non-compliance with clear-desk and clear-screen policies are recorded and action taken in accordance with a clearly defined consequences model.

17.28.3 Policy clearly states the requirement that all computers have screen-lock timeout capabilities with password reactivation.

17.29 Adequately secure areas (e.g., with barriers and locks, safes, screens not visible from public land) with high-grade utilities:

17.29.1 Power feeds and distribution, air conditioning and controls (e.g., fuses, monitoring and alarms for intruders, fire/smoke, water and power issues, CCTV, UPS.

17.30 An auditable redundancy strategy is in place to ensure uninterrupted availability of all electronic equipment. Redundancy strategy may include but need not be limited to:

17.30.1 An equipment replacement plan.

17.30.2 Readily available repair and replacement components and parts based on the equipment risk application supported by a well-kept and current inventory control.

17.30.3 High-grade supporting utilities such as:

17.30.3.1 Continuous and uninterrupted power feed and distribution.

17.30.3.2 Air conditioning

17.30.3.3 Availability and functionality monitoring.

17.30.3.4 Intrusion, fire/smoke, water and power failure alarms.

17.31 Technical architectures/designs provide for:

17.31.1 Multi-factor authentication or similar arrangements to strengthen identification authentication and access controls for high-risk systems, privileged functions etc. e.g., procedures for issuing, using, retaining, replacing and recovering secure systems.

17.31.2 Control access to networks, applications, data, VPN's and firewalls.

17.31.3 The safe storage, transportation and encryption of portable storage media (USB sticks, portable hard drives, tapes, paperwork).

17.31.4 An inventory, list or database of information assets, IT and technical systems including details (names and/or roles) of their owners, managed within IT inventory or management applications.

17.31.5 Project management manuals, methods, policies, procedures, guidelines and, forms.

17.32 Management information concerning the Information Security Management System (ISMS) is available and includes:

17.32.1 Budgets

17.32.2 Headcounts

17.32.3 Progress reports containing relevant metrics

17.32.4 Information risk and security strategies to mitigate the risk

17.32.5 Plans, policies, procedures and guidelines that governs the ISMS

17.32.6 Governance activities to check/measure, enforce and reinforce compliance

17.32.7 All Information Assets register with supplier detailed information

17.32.8 Suppliers List with contact details

17.32.9 Servers Specification

17.32.10 Software Asset Register

17.32.11 Software Configuration details

17.32.12 User Profiles and Access Lists to various Software Systems

17.33 A RACI chart is available that shows, for each key information risk and security-related process or decision, which functions, roles or people are Responsible, Accountable, Supportive, Consulted or Informed.

17.34 Information management system risks are identified and mitigated as an inherent component of the overall security risk management system, policies and procedures.

17.35 The information security policy (or policies) lays out and confirm senior management's commitment to:

17.35.1 The organisation's information security objectives

17.35.2 Continuous improvement of Information Security Management (ISM).

17.36 The Information Security Management System (ISMS) scope clarifies the boundaries of the certified ISMS in relation to the context or business situation of the organisation (e.g., certain business units, sites or departments), and its information risks and security requirements plus any imposed by third parties (e.g., laws and regulations).

17.36.1 Systems hosted by third parties on the cloud

17.36.2 Services provided by third parties, e.g., Internet Services

17.36.3 Systems on premises

17.36.4 User Support Contractor

Guidance:

Equipment specifications for procurement purposes - Systems Obsolescence

- In the era of Industry 4.0, big data and computing technologies are driving the future of manufacturing. While these innovations are extremely valuable for manufacturers, the increasing speed of technological change also means that equipment components are prone to quicker obsolescence.
- According to the definition from the International Institute of Obsolescence Management (IIOM), obsolescence is the unavailability of parts or services that were previously available, and usually occurs when the components of a system are no longer produced by the original equipment manufacturer (OEM) or when the latter is no longer in business. This means that when these components break or experience a malfunction, replacements can be hard to find.
- Obsolescence is the by-product of continuous technological advances and as such it cannot be eliminated completely, especially now that manufacturers are under more pressure than ever before to digitalise their facilities. However, plant managers should not feel forced to perform costly systems upgrades every time an obsolete component break.
- Obsolete does not mean useless or underperforming, and sourcing a like-for-like replacement can be quick and easy with the help of a specialised supplier. Additionally, in highly regulated industries such as nuclear and pharmaceutical manufacturing, upgrades also mean realms of paperwork and red tape, making like-for-like replacements the easiest choice.
- This is the basic idea behind managing obsolescence in a manufacturing facility—maintaining systems by sourcing obsolete components in a timely and cost-efficient way. With a proactive obsolescence management plan in place, legacy equipment can be perfectly integrated into a smart factory, allowing manufacturers to digitalise their plants while saving money and reducing their environmental footprint. Let’s see how in seven simple steps.

Step 1: System assessment

- To effectively plan, you’ll need to know the present state of your system by performing a comprehensive system audit. How old is your machinery and how long have its components been on the market already?
- Compare your answers with life expectancy data provided by the OEM to determine the life stage of your machines and their components, so that you can have a better idea of how long they will still serve you. Finally, make a list of components that are already obsolete or are about to be made obsolete by the OEM.

Step 2: Resource planning

- Strategic obsolescence management requires resources. Do you have a dedicated budget for periodic upgrades and last-time purchases? Can you afford to hire an obsolescence manager to help you keep track of components life cycles and plan repairs when needed?
- Most importantly: do you have partnering agreements with a reliable automation parts supplier? When obsolete components break, knowing who to call can make the difference between hours or weeks of costly downtime.

Step 3: Risk analysis

- Critical applications, which are essential to operate the entire system, are ones you should prioritise when putting together an obsolescence plan. If a component of these applications broke down, how much would downtime cost your business? Draw up a risk assessment form to decide whether you can risk them breaking down or whether preventive maintenance is the most convenient option.
- Analyse how worn their moving parts are, and research whether they are still available from the OEM or whether there are compatible products on the market. If they're already obsolete, contact a specialised supplier to get a quote. Since a failure of these components would impact the functionality of the overall system, timely replacement might be the way to avoid unplanned downtime.

Step 4: Shopping and stocking

- Industrial parts need to be grouped based on their risk of becoming obsolete. For components that are already obsolete, evaluate the possibility of stockpiling some spares while they are still relatively abundant on the market. For end-of-life (EOL) components, OEMs may send a last-time buy (LTB) notice and even provide special quotes. This might be the best time to squirrel away some spares.
- Do not forget that for larger spare parts you might need to have a dedicated a space in your warehouse. This space and its correlated costs must be accounted for in step two.

Step 5: The right supplier

- Based on your analysis of how critical a part is to your process, the speed at which it will wear and its risk of becoming obsolete, you should draw up a plan of where you can source these parts from and how quickly.
- For example, if a supplier doesn't regularly hold a specific obsolete VSD in stock, they'll have to source it from a third party, which could be located halfway around the world. Working with a specialised industrial automation parts supplier means you are safe in the knowledge that when a part does break down, you immediately know who to call to get your obsolete replacements quickly.

Step 6: Putting together a database.

- All the data collected so far should be recorded and safely stored. This information is invaluable and collating it into an easy understandable format could save precious time in case of breakage.

- This does not necessarily mean investing in an elaborate database. For small to medium plants, it can be enough to have a clear spreadsheet detailing the conditions of critical parts, their likelihood of breaking down, and the contact information of suppliers who have them in stock or can provide them quickly.

Step 7: Reviewing and updating

- Effective obsolescence management is a full-time job. It takes careful management to keep automated systems pitch perfect, which is the reason why larger businesses opt for hiring an obsolescence manager and sometimes even one or more last-time-buy professional purchasers who are responsible for managing EOL parts.

- However, smaller plants can go a long way by simply keeping their spreadsheets updated and organised. Make sure you subscribe to OEMs' newsletters to be notified when parts are discontinued and last-time-buys are available. Plan regular checks to update your spreadsheets, increasing their frequency for parts that are already visibly worn.

- By incorporating obsolescence management into maintenance plans, companies can minimise the impact of breakdowns, eliminating last minute repairs costs and saving money in the long run.

- Book of Obsolescence Management - Jonathan Wilkins (2016)

- System Specifications for procurement

- When writing a security specification consider the following headings:

TABLE OF CONTENTS

1. SCOPE

1.1 Introduction

1.2 Purpose

1.3 Applicability

2. APPLICABLE DOCUMENTS AND REFERENCES

2.1 Applicable Documents

2.1.1 External Documents

2.1.2 Internal Documents

2.1.3 Project Documents

2.2 References

2.2.1 External Documents

2.2.2 Internal Documents

2.2.3 Project Documents

3. REQUIREMENTS

3.1 System Definition

3.1.1 General Description

3.1.2 Operational Requirements

3.1.3 Maintenance Requirements

3.1.4 Security Requirements

3.1.5 System Diagrams

3.1.6 Interface Definition

3.1.7 Environmental Conditions

3.2 System Characteristics

3.2.1 Performance

3.2.2 Physical Characteristics

3.2.3 Availability

3.2.4 Maintainability and Reliability Requirements

3.3 Design and Construction

3.3.1 Materials, Processes, and Parts

3.3.2 Environmental Impact

3.3.3 Name Plates and Product Marking

3.3.4 Workmanship

3.3.5 Interchangeability

3.3.6 Safety

3.3.7 Human Performance / Ergonomics

3.3.8 Diamond Control

3.4 Documentation

3.5 Logistics

3.5.1 Maintenance

3.5.2 Supply

MPS 17 - Security Operations (Patrolling and Guarding)

Intent

To ensure that our security teams are effective, well trained, work to our code of ethics outlined in our corporate sustainability policies and are trained in and apply the Voluntary Principles on Security and Human Rights.

Required Actions

Fitness for Security Work

18.1 All security personnel (employees and contractors) will be required to be fit for service and pass the The Company medical fitness requirement.

Policies and Ethics

18.2 The Company operations will observe the applicable The Company Sustainability policies which provide a basis for ethical decisions in the conduct of security operations, and conduct a due diligence exercise annually to identify gaps in the application and execution of the requirements, supported by an action plan to rectify shortcomings. These include but are not limited to: Voluntary Principles on Security and Human Rights (VPSHR), Societal, and Health & Safety policies.

18.3 These policies and their application will form part of all security personnel's training.

18.4 Included in the training will be all identified stakeholders, including but not limited to:

18.4.1 Appointed private security providers.

18.4.2 Public Security providers assisting with the securing of the concession area.

18.4.3 Local community forums and/or members.

18.5 While the Public Security is not directly under The Company control, where they uphold the rule of law on our concessions, we will make them aware of our ethical approach and of the Voluntary Principles on Security and Human Rights (VPSHR).

Security Organisation and Reporting

18.6 The Risk Manager (Security) will report directly to the senior most executive at the operation (or delegate).

18.7 All The Company Security and Private Security contractors will be licensed and qualified in accordance with the local legislation for security.

18.8 The procurement of private security contractors will:

18.8.1 Comply with the VPSHR and relevant clauses of the International and/or the country of operation Code of Conduct for Private Security Providers.

18.8.2 Include as part of the contractual arrangement:

18.8.2.1 The ability to audit their payments to personnel, recruitment and training processes.

18.8.2.2 Their submission to annual auditing or due diligence as far as compliance with the VPSHR is concerned.

18.8.2.3 Their participation in the declaration of human right records as far as their employees are concerned, in accordance with the VPSHR requirements.

18.8.3 Require minimum levels of medical fitness which will be assessed annually.

18.8.4 Clearly define in the contractual agreement:

18.8.4.1 All required services, including the obligation to report security related incidents.

18.8.4.2 Agreed deliverables and timelines.

18.8.4.3 The obligations, roles and responsibilities of each party in terms of services to be provided and ethical obligations, including confidentiality requirements.

18.8.4.4 Processes for the management of the contracts including dispute resolution.

18.8.4.5 The obligation to comply with country based regulatory and legislative requirements, including company policies and procedures.

18.8.4.6 The obligation to comply/subscribe to the VPSHR.

18.8.4.7 Their obligation to comply with minimum training requirements as well as the conditions pertaining to that training, such as minimum entry level training requirements, annual refresher and developmental training requirements, where the costing of such training will reside and the record keeping and availability of training records.

18.9 Have a written protocol in place with public security that stipulates the model clauses recommended by the Voluntary Principles Secretariat. See Appendix 2 to Annex H.

18.10 The written protocol with public security may include but need not be limited to a formal contract, a jointly agreed procedure, signed-off and agreed to minutes of meetings and/or a memorandum of understanding.

Training of Security

18.11 Risk officers, including private security providers, will receive training appropriate to their tasks and satisfy the applicable local security regulations. In the absence of security regulations for licensing the training will include but need not be limited to:

18.11.1 Conflict resolution

18.11.2 Assertiveness in security

18.11.3 Duties of a sentry and post orders including search techniques applied

18.11.4 Patrolling techniques specific for the environment and threat

18.11.5 Use of radios and GPS (if issued)

18.11.6 The mining and processing of Diamonds – e.g. What they need to secure and how to dynamically assess risks to the process.

18.11.7 Voluntary Principles for Security and Human Rights

18.11.8 Supervisors training for Supervisors

18.11.9 Surveillance Monitoring

18.11.10 Risk Management and assessment (as it is core to the security function)

18.11.11 First aid training

18.11.12 Giving and taking verbal and written statements.

18.11.13 The Voluntary Principles on Security and Human Rights (VPSHR)

Firearms and the Use of Minimum Force

Community Engagement and Security

18.12 The Risk Manager - Security will work with the Community Social Responsibility team to ensure that Voluntary Principles on Security and Human Rights (VPSHR) and CSR programmes are aligned. The Security Team will assure this review co-ordination occurs at least annually.

Artisanal Mining

18.13 Where artisanal mining is present on a concession area the miners will be moved off the area in accordance with the relevant local laws or regulations and treated with respect for their humanity. *[Guidance: this is normally a Public Security task, upholding the rule of law.]*

18.14 Closing artisanal mining pits is a dangerous activity and all due care and precautions will be taken to ensure that they are clear of people before they are closed to protect The Company and its employees a sign off process will occur before pit closure including at least public security, The Company security, and the Mining or Exploration Departments.

18.15 There will be a process in place to inform artisanal miners of the illegality of their mining on the concession area and the implications of doing this. *[Guidance – this may be through the regular patrols of the concession area, community forums, the VPSHR stakeholder engagement or signage placed across the concession area.]*

18.16 The security risks and the consequences posed by artisanal miners to the organisation will be clearly reflected in the security risk assessment and risk mitigation strategy.

Guidance

- In new operations with significant artisanal mining or complex community relations operations should consider having a dedicated legal advisor supporting the communities and the security teams.

- Names of security officers contracted by the operation to render security services as per this standard are to be kept on record together with proof of compliance in terms of medical fitness, minimum training achievements, annual refresher training requirements, scholastic qualifications, and security clearance status. Verification that only those who qualify are deployed should be incorporated into the security reporting framework.

- Deployment records are to be submitted daily by the security service provider for analysis to ensure that only those security officers who are in compliance with the requirements stipulated in this LDCS are deployed.

- Any deviation from the approved list of security service providers employees should be pre-approved by the Risk Manager (Security) upon verification that all minimum requirements are met by the new appointee.

MPS 18 – Secure Transport and Logistics

Intent

To ensure that we minimise the risk to our people and product during shipment and have appropriate controls to maintain the integrity of the chain of custody.

Required Actions

19.1 An approved and signed off procedure that governs the manner in which product shipment must be conducted is in place, implemented and reviewed annually. As a minimum requirement the procedure should:

19.1.1 Contain standard operating procedures for the movement of diamond shipments.

19.1.2 Define the roles and responsibilities of product movement team members.

19.1.3 Stipulate the minimum standards in terms of the maintenance of the core product movement team.

19.1.4 Govern the scheduling of shipments to ensure timeous deliveries in alignment with respective production cycles.

19.1.5 Allow for variation of scheduling routines to mitigate identified risks.

19.1.6 The minimum training requirements for product shipment team members.

19.1.7 Contain guidelines on how to maintain product movement confidentiality requirements, including but not limited to control measures to ensure the confidentiality of product movement information and the utilisation of security encrypted protocols when communicating prior to, during and/or after product movement.

19.2 In all cases, local regulatory or legal requirements like the Kimberley Process will be met regarding the movement of Diamonds.

19.3 A product shipment risk assessment will take place if there are major changes in the threat to shipments, the process or the provider. It will be reviewed annually to assess the effectiveness of security controls applied to the Product Shipment Process.

19.4 All persons involved with the Product Shipment Services must comply with the country of operation's licensing requirements and be equipped and qualified for the activities associated with product shipments.

19.5 If any part of the product shipment process is outsourced a written protocol, procedure, contract or agreement must be in place that regulates the relationship between and its shipment contractor or supplier, and the document must be established in accordance with The Company procurement principles.

19.6 Any product shipment contractor used by The Company is subject to appropriate due diligence to ensure its company directors and owners are professional and pose no risk to The Company, including reputational through compliance to the UN Voluntary Principles on Security and Human Rights and the Precious and Semi-Precious Stones Protection Act - Botswana.

19.7 Insurance should be in place for Product Shipment. Where the Contractor provides these they are to be approved by The Company Chief Finance Officer and advice obtained on whether the coverage and clauses are correct and aligned with The Company's insurance arrangements before engaging any contractor.

19.8 As part of Security Governance, the insurance policy must be reviewed annually to ensure:

19.8.1 That is not underinsured

19.8.2 That the insurance agency or underwriter agrees with security measures, and/or alternatively that the minimum-security requirements of the insurance schedule is complied with each time that product shipment takes place.

19.8.3 For each shipment that takes place, there must be measures in place to ensure that shipment complies with the shipment insurance security requirements.

19.9 The Risk Manager (Security) will develop a protocol together with the product shipment contractor and/or police in the case of The Company that governs the response to robbery/hijack whilst The Company personnel are present and such protocols will be rehearsed and integrated into training of those The Company personnel. This training will happen at least annually for all such exposed personnel.

Requirements of a Product Shipment Contractor where used:

19.10 The product shipment contractor will:

19.10.1 Comply with the minimum criteria for shipment contractors determined by the organisation or set by the country authorities.

19.10.2 Utilise pre-approved secure storage facilities during product shipment.

19.10.3 Employ qualified personnel that are certified and trained in their duties and registered as such with a regulator if required.

19.10.4 Have reliable communications between the vehicles they use and their operations centre and that this centre operates throughout any shipment.

19.10.5 Have a protocol for managing a diversion of the product to an alternate airport or holding area whilst in transit from mine to secure holding facility.

19.10.6 Have an established communications plan and a written protocol in place with the designated public law enforcement agency that stipulates the roles and responsibilities of involved parties and stakeholders in the event of robbery/hijack; and

19.10.7 Allow auditing of their operations for compliance to these standards by The Company from time to time but in any event, every three years or as part of the procurement process, whichever is sooner, and that provision for such auditing is included in the contract when renewed.

Surveillance and the Chain of Custody

19.11 The sealing of the product into tamper-resistant containers ready for shipment will be under surveillance and the footage of such preparations for shipment will be reviewed and retained for comparison.[14]

[14] Subject to data protection guidance, such footage will be retained at the discretion of the Security manager and Surveillance leader but should include at least the past four shipments.

19.12 The handover of the product shipment will be witnessed by a member of the Botswana Police Diamond and Minerals Protection Unit, one The Company Security person in addition to the person involved in the handover. Surveillance coverage is considered as being a witness to a hand over. Where the process does not allow this the movement of the tamper-resistant containers out of the sort-house and into the first transport will be witnessed.

19.13 The receipt of product shipments and their initial processing and entry into the stock control/tracking system is a higher risk activity and will be subject to surveillance. The surveillance footage of such activities will be reviewed and retained for comparison.[15]

Guidance – Reserved

[15] See footnote above.

MPS 19 - Surveillance and Analysis

Intent

To ensure we optimise the use of CCTV Surveillance and other security systems, through appropriately selected, trained, and motivated personnel that can assess and respond to security alarms and incidents efficiently, by being focused on the risks.

Required Actions

Surveillance Personnel

20.1 Evidence that the use and placement of surveillance cameras are risk based and suitable to meet the identified security need is available. Such evidence may include amongst others a camera risk assessment for each area. Based on the risk and the security need (Defined objectives) that was identified, cameras will be identified and placed considering, but not limited to:

20.1.1 Environmental conditions

20.1.2 Recording capability

20.1.3 Image quality

20.1.4 Level of detail required, i.e., zooming capabilities.

20.1.5 VMD requirements

20.1.6 Redundancy requirements, i.e., replacement protocols in the event of malfunctioning or when service duration has expired.

20.1.7 Forensic integrity requirements

20.2 The Risk Manager (Security) is to ensure that surveillance personnel are dedicated to the surveillance role and are directly and specifically employed to fulfil the surveillance task and are not general security officers.

20.3 The Risk Manager (Security) will maintain a profile for each surveillance operator reflecting results of aptitude and competency, other tests, training completed and standard and frequency of surveillance reporting.

20.4 Transfer into or out of the surveillance function from any other function is actively discouraged and is subject to approval by the Risk Manager (Security). in consultation with the relevant Risk Coordinators.

20.5 Effective surveillance requires knowledge of processes, physical layout of the facility and the behaviours of personnel working in high-risk areas. Surveillance personnel will receive training to allow them to gain this knowledge.

20.6 All surveillance personnel will be conversant and compliant with the following and confirm as such in writing at least annually:

20.6.1 Local legislation regarding surveillance and data protection and The Company Data Protection Policy, and;

20.6.2 That they know and undertake to adhere to the requirements for ethical use of the surveillance system.

Security for the Surveillance Cell

20.7 Surveillance will be conducted from a secure facility.

20.8 The areas where surveillance control data or imagery is stored or transmitted such as server rooms and cabling should be subject to the same security controls as the surveillance facility.

20.9 Access to surveillance and control facilities is to be limited to surveillance staff and company personnel approved by the Risk Manager (Security)from time to time. It should not ordinarily allow security or operations personnel in. Records should be maintained of access to the surveillance facility.

Surveillance Standard Operating Procedures

20.10 Standard Operating Procedures will be established that allow the application of quality management and consistency of execution. As a minimum SOPs will adequately address the areas noted in the generic SOP document:

20.10.1 Responsibilities.

20.10.2 Shift Change Routine.

20.10.3 Risk Management.

20.10.4 Communication and response.

20.10.5 Recording observations, incidents and events.

20.10.6 Alerting and escalation of events.

20.10.7 Access and Privileges; and

20.10.8 Data and Assurance.

20.11 The Risk Manager (Security) is to implement a Quality Management Process to ensure surveillance systems are being utilised effectively and ethically. As a minimum requirement the following aspects are to be measured and monitored:

20.11.1 Daily, weekly and monthly review of the quantity and quality of the reports generated by each member of the surveillance team.

20.11.2 Control over the surveillance function and the quality assurance over the effective utilisation of the surveillance function must be conducted by the Risk Coordinator (Operational Support) within the operation, reported directly to the Risk Manager (Security) and secured within the security database.

20.11.3 The planning of surveillance activities with clear evidence that a risk-based approach is followed to inform priority observations.

20.11.4 The type and nature of surveillance activities, including but not limited time spent on non-surveillance activities.

20.11.5 Scheduled plant visits by surveillance officers to familiarise themselves with plants, facilities and processes and to establish camera-area orientation.

20.11.6 Hand-over and take-over of shift duties.

20.11.7 Reporting and follow-up/closure of incidents.

20.11.8 Activities related to the monitoring of diamond recovery processes, the identification of malicious and non-malicious vulnerabilities and reduction/elimination of process anomalies as a direct result.

20.11.9 Identification of surveillance footage to be reviewed and the actual reviewing, record keeping and quality management thereof.

Surveillance Response, Recording and Reporting

20.12 Where there is any breach of the safety standards and it is observed in real time, the operator must intervene immediately to prevent injury and a record of such must be kept, in the official incident management kept by security.

20.13 Any safety or security incident whether observed in real time or focussed review must be recorded in the incident management system by the individual operator that observes the event.

20.14 Incident reports will be generated for every instance of a break into the diamond recovery circuit in high-risk areas. Examples of such interventions into the diamond recovery circuit include:

20.14.1 Spillages.

20.14.2 Clearance of blockages in the recovery process.

20.14.3 Maintenance events – unscheduled and scheduled.

20.14.4 Sampling and tracer (DMS and optical sorting) testing.

20.14.5 Process anomalies/operational failures.

20.14.6 Machine and/or equipment purging.

20.14.6.1 No human interface in/on diamond recovery machines, equipment, machine components and/or auxiliary equipment, in high-risk areas should take place unless clear evidence is provided that the diamond recovery machines, equipment and/or auxiliary equipment has been purged from any and/or all diamond containing material. If this ruling is not complied with, the incident should be reported and escalated in accordance with a written protocol.

20.14.6.2 Should the purging of diamond recovery machines, equipment, machine components and/or auxiliary equipment in high-risk areas not be possible prior to human interface with such diamond recovery machines, equipment, machine components and/or auxiliary equipment, authorization should be obtained through the submission of a deviation request as per the change management process.

20.15 Incident reports for high-risk interventions into the diamond recovery circuit will clearly reflect evidence that incidents were observed by surveillance and where necessary, and in according to pre-set criteria, incidents will be posted for second tier review by a dedicated team of reviewers.

20.16 Should there be clear evidence that high-risk interventions into the diamond recovery process were not observed by surveillance, an enquiry and/or investigation should be initiated to determine the reasons why surveillance was not conducted and to implement measures to prevent a re-occurrence.

20.17 The following requirements must be met with regards to the second tier reviewing of incidents:

20.17.1 The reviewing process must be governed by a procedure that includes but need not be limited to:

20.17.1.1 The type of events, actions or circumstances that will trigger video review to ensure consistency in application.

20.17.1.2 The formal record keeping of review findings, follow-up action and feedback.

20.17.1.3 The quality assurance, monitoring and closure of reviewed incidents.

20.18 There is a methodology or system in place to monitor exposure of product to human contact, with ongoing intervention to reduce such, supported by clearly displayed metrics to measure the effectiveness of the interventions.

20.19 Protocols will be developed in tandem with operations to ensure that surveillance is informed of interventions into the diamond circuit before the interventions happen.

20.20 Records of the observations must denote who was involved, what happened; where it happened; when it happened; why an event happened and any notable environmental conditions at the time of the event.

20.21 Incident reporting officers are monitored and supported on an ongoing basis, and incident reporting is monitored to ensure incident are complete accurate and reliable so as to ensure the integrity of reported data.

20.22 Mechanisms are in place to ensure that all incidents affecting the security of the organisation or that may lead to loss to the organisation are reported.

Non-Compliance events are clearly defined in the operation’s SOPs comprehensively communicated and clearly displayed, with clearly defined guidelines indicating under which circumstances security personnel should intervene, how to intervene and how to escalate incidents when a non-conformance event and/or security control failures in high-risk area are observed. Limits of authority should be clearly specified *Access to Imagery and Data-Protection*

20.23 The Risk Manager (Security) is to ensure that procedures are in place governing access to imagery and data. Reference will be made to ensure that data protection protocols are in place stipulating how and to which location the data is transferred. These procedures must include:

20.23.1 Authorisation,

20.23.2 Dissemination, and

20.23.3 The recording of decisions and access granted.

20.24 The Risk Manager (Security) must grant authorisation to internal stakeholders to access footage and security data, and records of such access will be kept in Perspective and the Risk Co-ordinator (Operational Support) informed. The information recorded should specifically mention:

20.24.1 The date of disclosure.

20.24.2 Who it was disclosed to; and

20.24.3 Why it was disclosed.

20.25 Data and CCTV footage gathered by the surveillance function is sensitive and is classified Confidential.

20.26 Procedures include the data storage protocols, and the way in which access to data is controlled.

20.27 Detail regarding correct use of surveillance systems such that it could not damage the integrity, or the professional reputation of The Company will be included in SOPs and training material.

20.28 All people entering the mining area, including but not limited to personnel, contractors and visitors will be made aware and will provide written consent to monitoring by Surveillance including the use of CCTV.

20.29 Transfer of data and imagery between The Company companies must be in accordance with any legal requirements and contractual provisions between entities be in place before data is transferred.

20.30 Data and imagery should be stored and retained for a period to fit with operational requirements,[16] unless legislation directs a lesser period.

20.31 Data and imagery of high-risk activities such as interventions into the diamond circuit should be stored so that a library can be made up for future detailed comparison of the same activity. This is to provide a sample of efficient and correctly conducted activities with which to compare future similar activities for compliance and efficiency.

20.32 Data and imagery referring to incidents should be backed up and stored separate from the surveillance suite for as long as local legislation and capacity allows.

External Liaison

20.33 A formal list of external liaison contacts will be compiled and maintained by the Risk Manager (Security) for all The Company operations (Karowe Diamond Mine and Corporate Office, Diamond Technology Park).

20.34 Liaison will be structured in accordance with the threat indicators and the information collection plan.

[Guidance for External Liaison – such liaison contacts will assist the Risk Manager (Security) form a picture of the local threats and providers of assistance and as such may include local police commanders, peer group companies, security providers, customs officials etc. use of such external liaison should be systematic and due care taken in recording any information including allegations of wrongdoing from uncorroborated sources. Stakeholder identification could be part of the VPSHR process for stakeholder identification.]

[16] This is likely to be 30 days but, subject to local legislation, may be longer to cater for longer sales cycles.

The above information could be included in a business environment scan. The business environment scan forms part of the risk management process is done once and reviewed annually and forms the basis for threat identification.

Guidance

- Where possible surveillance should be offsite – at least for review and assurance.
- Such off-site assurance should report operationally to the Risk Manager (Security) but for independence to the Chief Risk Officer and MD The Company.
- High-risk activities should be clearly defined such that a norm can be established. A norm will provide for consistent actions and movements when people interact with diamond material. This will assist the application of the surveillance control.
- Where regular interventions to the diamond recovery process take place such as sampling, consideration should be given to the use of photographs on a single point brief of a correct authorised way to conduct a sample so that the operator is aware of the correct method and consistently faces the same way with hands in the same position and completing actions in the same order.
- The surveillance philosophy is based on pragmatic approach centred around a three- tier structure namely:
    - First Tier
    - Second Tier
    - Third Tier
- First Tier:
    - This is the first level of surveillance which focus on general surveillance of risk areas. This Level undertakes routine remote plant/premises patrols and remote escorting and consists of dedicated, focused and/or real time surveillance.
- Second Tier:
    - This is the second level of surveillance which concentrates on identified specific risk elements for detailed information. These operators target individuals or a group of people (regarded as Hot People) at risk areas (regarded as Hot Places). They also target risk processes (regarded as Hot Process) and detect any risk behaviour at identified areas or process. This second level of surveillance is triggered by first tier surveillance, supports, consolidates and acts as an audit structure of First Tier. This level has a responsibility to archive any deviations or abnormalities on a separate storage material which must be revisited whenever need arise.
- Third Tier:
    - This Level of surveillance consist of management and is responsible for system administration and configuration as well as auditing, including remote assurance.

MPS 20 - Resilience and Recovery

Intent

To be a resilient business; we have plans and the capability to identify, mitigate, control, and recover from incidents that can disrupt our business.

Required Actions

Major Risks

21.1 Based on The Company's Business Continuity Management (BCM) policy and procedures, all departments are to complete a Business Continuity Plan that assesses the six pillars of business continuity, namely:

21.1.1 Functions

21.1.2 Skillsets

21.1.3 Equipment

21.1.4 Documentation

21.1.5 Suppliers

21.1.6 IT Systems

21.2 Included in the BCP and BCM software (BCM Toolkit) is also the risks associated with the resilience of that department. These risks are to form part of the risks to be properly assessed, recorded in the Governance, Risk and Compliance software (CURA), so that risks contained in the BCM Toolkit are brought into the departments risk register and BCM Module

21.3 Major risks are identified as part of the risk management process and not in isolation.

[Guidance: These risks should be identified as a normal part of risk assessments where a systematic approach is followed to identify all risks. If this is not done, some risks may be overlooked.

Major risks include but need not be limited to incidents that can impact or disrupt the business in a major way.]

21.4 Major risks are clearly defined in the risk management procedures.

21.5 Trigger action response plans (TARPs) have been compiled for each major risk that was identified. (Trigger action response plan)

21.6 The TARP forms the underpinnings of the business resilience plan that:

21.6.1 Identifies the critical equipment and/or spares needed to mitigate the major risk.

21.6.2 Identifies the key internal and external stakeholders that are involved in the event of major risks materialising.

[Guidance: such stakeholders can include customers, investors, media, local communities, government, employees, contractors, NGOs and other with an interest in the operation.]

21.6.3 Detail the key actions to take in the immediate aftermath of an incident

21.6.4 Identifies personnel to manage major risks once they materialise.

21.6.5 Identifies the training requirements, including a training schedule involving all stakeholders, personnel and emergency services that will be involved should the risk materialise.

21.6.6 Details all resources (budgetary, time and equipment) for the maintenance of the plan and associated training.

21.6.7 Explains the manner in which responses will be rehearsed, and actual incidents will be reviewed and shared in an attempt to learn from it and improve responses and/or prevent it from recurring.

21.6.8 Outline how incidents are used to improve The Company group preparations for other incidents and share learnings with other The Company operations.

21.7 Operations will include in their planning and documentation the response to security events appropriate to the identified major risks. As a minimum this must include:

21.7.1 Response to natural disasters

21.7.2 Response to cybercrime and cyber terrorism

21.7.3 Response to civil emergencies, strikes and similar actions

21.7.4 Response to pandemic threats including Covid19

21.7.5 Response to compliance failure

21.7.6 Response to robbery, violence, or the threat of violence.

21.7.7 Response to catastrophic failure of systems or technology

21.7.8 Response to supply chain failure

21.7.9 Consideration for the security of product during site evacuations including fire.

21.8 The relevant employee should be familiar with and incorporate the provisions for Business Resilience and Recovery Planning detailed by the Business Units management system and supporting documents.

21.9 Critical spares will be provided by various Departments. These spares will be listed by the Procurement team and verified by The Company Management and maintained to ensure their integrity is kept intact.

Guidance – Reserved

Proof

MPS 21 – Documentation and Metrics

Intent

To ensure that all documents, records and data relating to Security and Security Risk Management are fit for purpose, controlled and accessible by the appropriate personnel. They will describe the operations and provide the basis for the management of change, audits and operational metrics.

Required Actions

22.1 Security framework documents will be prepared in a style appropriate for their intent and intended audience.

22.2 An effective document control process will be in place that describes:

22.2.1 Version control and the communication and control of changes;

22.2.2 Distribution, access and use;

22.2.3 Storage and preservation;

22.2.4 Retention and disposal.

22.3 The security framework will be appropriately documented. As a minimum this will require:

22.3.1 Security Charter and/or Mandate

22.3.2 Security Strategy Plans for a 3-5 year period

22.3.3 Resilience Plans for each The Company operation;

22.3.4 Detailed Standard Operating Procedures for all high-risk diamond handling areas including mining areas, process plants, recovery plants, sort-houses, sales and auction rooms;

22.3.5 Security plans for each operation;

22.3.6 Detailed diagrams and plans for technical security systems including:

22.3.6.1 Power inputs including provision for UPS and surge protections

22.3.6.2 Technical diagrams and designs to enough detail such that works can be commissioned effectively and form the basis for the management of change.

22.3.6.3 Technical yearly plan for maintenance and projects

22.3.6.4 Typical panel layouts and wiring

22.3.6.5 Detailed technical product specifications

22.4 Metrics will be developed for Security activities so that the Managing Director, General Manager and other identified key stakeholders can see that it is managed properly and effectively. Guidance: such metrics are likely to include:

22.4.1 Monthly Security Operations Report (consolidated executive management security report for both Karowe Diamond Mine and the Corporate Office in Gaborone)

22.4.2 External Security Assurance Provider Reports (for both Karowe Diamond Mine and the Corporate Office in Gaborone)

22.4.3 Operational Risk Management Plans (for both Karowe Diamond Mine and the Corporate Office in Gaborone)

22.4.4 Security Risk Register (as extracted from the Governance, Risk and Compliance software tool, CURA)

22.4.5 Staff availability and deployment activities

22.4.6 Budget compliance

22.4.7 Incidents reported by category

22.4.8 Incidents investigated and outcomes

22.4.9 Staff development

22.4.10 Current and future projects

22.4.11 Technical systems as below

22.4.12 Non-compliance to procedure events in high-risk diamond areas such as recovery or sort-houses

22.4.13 Number of complaints received from the local communities about the security personnel

22.5 Metrics for Technical Security Systems will be used and include as a minimum:

22.5.1 Availability of all systems (% or #)

22.5.2 The number of server restarts (and why)

22.5.3 Maintenance completed (Planned vs Unplanned)

22.5.4 End of life for key equipment (6months, 1yr, etc.)

22.5.5 Key faults for the period

Metrics

22.6 Security metrics will be developed to suit the operations (both at Karowe Diamond Mine and the Corporate Office in Gaborone) and should focus on measuring the desired outputs. Where possible reporting should be automated and be readily available.

Guidance – Reserved

The availability of complete and accurate documentation under the Records Management Program allows to:

- Protect the legal and financial rights of and of individuals directly affected by activities; and

- Preserve institutional memory so that informed decisions are possible and thus facilitate action by The Company and contractor officials and their successors.
- Archive storage to store important documents in a professional and secure environment, freeing up space within office.
- The Document Centre shall be a safe storage of all documents owned by The Company.
  - Legal requirement - Records is legally obliged to archive
  - Records management is the law -- not just good business practice.
  - ISO certification demonstrates that uses one of the recognised ISO management systems. - ISO 27001 certificate

MPS 22 – Investigations into Suspected Wrongdoing

Intent

To thoroughly investigate incidents of suspected wrongdoing while ensuring that any information or evidence collected can be used by subsequent internal or criminal investigations as required. Incidents will be recorded, notified to the appropriate people and investigated correctly to learn lessons for improvement

Context - Investigations into suspected serious wrongdoing [i.e. significant financial loss or the catastrophic failure of internal controls] must be treated differently from a simple inquiry. The outcome of investigations can include dismissal, public trial, imprisonment for offenders, legal reviews and media attention; as a result, management of investigations requires particular attention to local laws, employment regulations, labour relations consequences, Human right violations and the preservation and continuity of evidence.

Required Actions

23.1 The organisation should:

23.1.1 Develop a procedure that governs the way in which security investigations are to be conducted, including the administration processes and documentation requirements associated with it.

23.1.2 Obtain management approval and sign-off for the procedure that governs the way in which security investigations are to be conducted.

23.1.3 Publish the procedure the way in which security investigations are to be conducted on the internalised document repository.

23.1.4 Communicate the procedure that governs the way in which security investigations are to be conducted.

23.1.5 Implement the procedure that governs the way in which security investigations are to be conducted by establishing a monitoring capability to verify implementation.

23.1.6 Review the procedure that governs the way in which security investigations are to be conducted continually to ensure alignment with business requirements.

23.2 An escalation procedure and matrix should be included in the procedure that governs the way in which investigations are to be conducted to inform the escalation process for significant Security events.

23.3 The line manager of the area impacted by the incident is accountable for producing this notification to the general manager.

23.4 All incidents of failures in Security will be recorded in the information reporting system and used for subsequent analysis.

23.5 Where general issues are identified that lead to losses such as lower numbers of quality Diamonds than expected, less diamond specials than expected, smaller size distributions than expected by the block model and whose root cause is unknown the issue will be escalated to the General Manager and Managing Director as soon as practical and an appropriate ad hoc working group convened to identify next steps and root causes.

23.6 Security incidents other than those involving Diamonds, such as theft of company fuel, should be treated in similar ways.

23.7 In all cases investigations and inquiries will be fair, objective and thorough, they will:

23.7.1 analyse the root cause of incidents,

23.7.2 document the investigations process,

23.7.3 preserve the continuity of evidence,

23.7.4 document the investigation results and any follow-up improvement actions.

Guidance – Reserved

- It is essential to cover Investigations Philosophy which covers:
    - Human Resources Investigations.
    - Operational or Security Procedural Breach or Failure.
    - Suspected Malicious Act.
    - Background or Security Clearance Investigations.
    - Due Diligence Investigations.
- It is essential to highlight on Investigative process and elaborate on different stages of investigations, e.g., Preliminary Investigation which is an initial fact-finding stage of an investigation and is usually performed at the scene of the incident and may be performed by a patrolling Security Officer or in high-risk areas a Team Lead.
- Follow-Up or covert Investigation which is the investigative process that is performed by the Specialist Investigator, possibly in conjunction with relevant law enforcement representatives and subject matter experts.
- For a well-coordinated investigation, before investigation takes place an investigation strategy should be agreed with the Head of Department. The agreed investigative strategy will be captured in a document outlining the scope of the investigation.
- Investigation should be initiated with the formal written authorisation of the Head of Department. Such authority should be retained within the case file.
- Individuals implicated in an allegation of wrongdoing must not conduct, or be involved in the direction of, an investigation that relates to them.
- Working with Government Law Enforcement Agencies
    - Head of Department must approve all operations designed to collect information that require working closely with Government Law Enforcement Agencies.
    - The Chief Risk Officer or Managing Director will also be consulted in the early stages of planning for any such potential operations and in all cases before they happen.
    - Head of Department must approve all liaison engagement with other Diamond Security Companies and Government Enforcement Agencies.
    - Head of Department to organise and conduct Environmental Scan every two years utilising the PESTEL and SWOT philosophies.

MPS 23 – Audits and Review

Intent

To confirm the efficient application of this Standard at all The Company operations and the continued relevance of the Minimum Performance Standards.

Required actions

Audits

24.1 The Company workplaces will carry out regular planned area inspections, reviews and audits at frequencies appropriate to the risk profile of the area being reviewed.

24.2 At planned intervals, operating sites will internally evaluate and report on the effectiveness of controls for significant Security risks.

24.3 Periodic external independent audits and reviews will be planned and undertaken for all operating sites. Audits and reviews will be conducted by suitably trained, experienced and independent people.

24.4 Operating sites will have a systematic process to manage issues and opportunities identified during audits and reviews.

24.5 An annual audit plan approved by the Chief Risk Officer will be available and administered by the Risk Manager – Security detailing and tracking all reviews and audits for the year.

Management Review of this Security Framework

24.6 The Company operating sites will complete security framework reviews at planned intervals. The intent of these reviews is to determine if the Security framework is 'fit for purpose' for the operation. Reviews will consider:

24.6.1 Suitability of Security policies, strategies and system components based on feedback from end users

24.6.2 How effectively risk is managed at all levels

24.6.3 Performance - Security trends, objectives and targets

24.6.4 Results of internal audits and other evaluations of compliance

24.6.5 Follow-up actions from previous management reviews and any other recommendations for improvement;

24.6.6 The status of corrective and preventative actions

24.6.7 How changing legal and other obligations are managed including communications from external parties

24.7 The review will identify areas for improvement and clearly state:

24.7.1 Reasons for change

24.7.2 Extent of change (including what is redundant and how it will be removed)

24.7.3 Timeline for change

24.7.4 Resources and accountability for change

24.7.5 Expected measurable benefits from the change

24.8 Records of completed management reviews will be retained, with relevant outputs communicated across The Company as appropriate.

Guidance - Reserved

MPS 24 – Security Information Management and Analysis

Intent

The Company is in an advantageous position with respect to Diamond Intelligence in that the Government of Botswana has a very strong Criminal Intelligence capability due to the Strategic importance of the Diamond Industry for Botswana. It is important that The Company's Security Team plays a supportive role to this Government capability and that is then the intent of this MPS.

Required Actions

25.1 The Company should have an internal capability to support the initiatives of Government Diamond Intelligence activities

25.2 Formal and regular interactions with Government and Local Authorities should be maintained and record kept of all interactions.

25.3 Formal meetings should be held at least once per quarter with Government Intelligence structures to discuss matters of mutual interest.

25.4 The MD The Company should be briefed in detail on the discussions during these meetings.

25.5 Regular interactions (at least monthly) should be maintained with other diamond operations in the region and a formal documented meeting should be held at least once per quarter.

25.6 The Risk Manager (Security) should attend all the meetings with respect to intelligence and investigations and brief the General Manager on a need-to-know basis.

25.7 Persons assigned to the intelligence support activities should clearly understand that they do not have certain jurisdictions outside of the operational area of the mine and should therefor be careful to act within the legal framework of the country.

25.8 The security incident reporting system should be analysed on a continuous basis to determine suspicious activities of persons. Specific attention should be directed to persons that repeatedly contravene operational procedures.

25.9 Other systems like the access control system, seal management, cctv, process maintenance etc should be cross referenced during this analysis these investigations.

Guidance:

What is Intelligence?

Intelligence is the umbrella term referring to the range of activities – from planning and information collection to analysis and dissemination – aimed at maintaining or enhancing relative security by providing forewarning of threats or potential threats in a manner that allows for the timely implementation of a preventive policy or strategy.[17]

The term "intelligence" often conjures the practice of espionage, thoughts of illicit or covert activities. This is not the context in which the term "intelligence" it is being utilized or referred to.

[17] Peter Gill & Mark Phythian - Intelligence in an Insecure World – Polity Press 2006

The term "intelligence" here should be considered as the sum total of two very distinct actions occurring in harmony with each other.

Information + Analysis = Intelligence

"Though often used interchangeably and incorrectly, there is a difference between information and intelligence. Unprocessed information helps raise awareness and understanding. When this information is analyzed and evaluated, it becomes intelligence. Intelligence provides situational understanding that enables better decision-making. Information plus analysis equal intelligence. [18] *"*

Being Intelligence Led is a process that will provide for the Security Department at the operational level to achieve maximum effectiveness. It provides for an encompassing organizational approach leveraging on numerous streams of information allowing for timely and tactical decision-making and paves the road for future strategic efforts to maximize resiliency.

Understanding the Intelligence Cycle[19]

In efforts to achieve internalized resilience, one need to fully understand the process, which must be followed. The process utilized to achieve this goal is referred to as the Intelligence Cycle. These very basic steps must be adhered to which will provide our Security Efforts to be truly and effectively Intelligence Led.

The Intelligence Cycle has four Key Processes

1. Requirements & Planning
2. Collection
3. Exploitation & Analysis
4. Dissemination

Requirements & Planning

As with any investigation, a starting point is required. The basic questions that always must be asked and determined are referred to as "W-5" — Who? What? When? Where? Why? (…And potentially the most important and evasive question to be answered is How?)

The answers to the specific questions will also be utilized as the starting points for identification of your respective intelligence needs into requirements of your respective Security Unit. These specific points will formulate the specific framework for decision makers who will determine and establish the Essential Elements of Information, and the planners and the intelligence staff. Typically, an individual is assigned as the Intelligence Resource of the Security Team and will be responsible for generating the Intelligence Requirements specific to the Business Unit, driving the production process.

Once the Intelligence Requirement is defined, spawned from internal or external vulnerabilities, potential threats or pressures, is then transferred into a Collection Plan. A specific individual quality trait of the Security Intelligence Resource is to identify the type of person will determine whether the intelligence produced is responsive to the user's requirements. Where intelligence is playing an increasingly important role, the focus is maintained primarily on the reduction of risk through the identification of potential vulnerabilities Government intelligence requirements are

[18] US Department of Justice – Global Justice Information Sharing Initiative "Navigating your Agency's Path to Intelligence Led Policing" April 2009

[19] The Intelligence Cycle White Paper – Bob Foose Techwriter.net 2006

expressed in terms of foreign threats to national or international security. In the business arena, where intelligence is playing an increasingly important role, requirements will generally be expressed in terms relating to individuals or groups involved within the illicit diamond trade.

Planning encompasses the entire intelligence process, beginning with the threat assessment phase and culminates with the delivery of the finished intelligence products. Plans are generated that are responsive to known or anticipated intelligence requirements.

Collection

The collection requirement specifies exactly how the intelligence service will go about acquiring the intelligence information the customer needs. It is normal for several players in the intelligence community to be involved in formulating collection requirements. Collection requirements may be managed by a group of specialists acting as liaisons between users and the collection resources. In non-government organizations collection management may be relegated to one person or team within an intelligence or operational security unit.

Collection requirements management entails much more than simple administrative duties. It requires analytic skill to evaluate how well the user has expressed the need; whether the collection assets are able to obtain the identified information, and how the collected information reaches the intelligence analyst.

Information from open sources are often a valuable collection resource in the business environment, including corporate publications, advertising, newspapers, periodicals, academic journals, foreign and domestic broadcasts, official documents and other published material. Analysts should not participate in any unlawful covert and or clandestine resources while performing this important collection task.

Exploitation & Analysis

Exploitation and analysis involve a series of mental operations various types of collected information or data with close examination of related items of information to determine the extent to which they confirm, supplement, or contradict each other, and thus establish probabilities, relationships, and conclusions. Analysts in all operational programs use their knowledge of regional, national, and global trends to assess the quality of all types of information gathered, and organize it into a responsive, useful intelligence product.

The purpose of intelligence analysis is to reveal to a specific decision maker the underlying significance of selected target information. Frequently intelligence analysis involves estimating one possible outcome, given the many possibilities in a particular scenario. This function is not prediction although in some cases it might be seen as such. The analysis typically can involve forecasting, which requires the analyst to make explicit statements about the degree of confidence held in a certain set of judgments. There are different levels of analysis associated with the production process, usually with results in corresponding levels of conclusions.

In intelligence analysis, the analyst typically does not have direct access to the observable subject, but, instead, gathers information from a variety of sources then proceeds to generating tentative explanations for a subject activity, event, or phenomenon. Each hypothesis is examined for plausibility and compared against the acquired information, in a continual process toward reaching a conclusion. Often the intelligence analyst tests several hypotheses at the same time, generating potential scenarios, and testing each using a rigorous mental processes, subject domain knowledge, experience, and a variety of other associated background "skills."

The successful intelligence analyst brings to the discipline:

- Certain requisite knowledges and abilities,

- Has necessary aptitude for specialized training,
- Can perform the specific tasks associated with the job, and
- Exhibits personality traits compatible with intelligence analysis work.

This profile is valid in any setting of intelligence activity.

The previously described steps of the cycle are necessary precursors to intelligence production, but it is only in this step that functionality of the whole process is achieved. Production results in the creation of intelligence, that is, value-added actionable information responsive to the user's needs. In practical terms, production refers to the creation, in any medium, of either interim or finished briefings or reports for use by other analysts, decision makers, or policy officials. The general production principles apply to both government and private sector intelligence operations.

Reporting and Dissemination

The production of intelligence is without relative value unless it is timely and reaches the prospective users in a form that allows exploitation of the intelligence. The business environment today is extraordinarily dynamic, with the result that information and intelligence is time sensitive, at highest value at the time of acquisition and depreciates rapidly from that moment. Actionable intelligence is perishable, although it may serve well as historical information too. The key, then, is expedited production and dissemination for action.

The intelligence process does not end with delivering the product to the customer. Instead, it continues in with dialogue between producer and user. If the product is to be useful, dissemination involves feedback. Intelligence producers need feedback from end-users.

They need to know what is useful and not useful to meet the intelligence requirements. Then producers can modify their practices to further develop those activities that served the user well and improve or eliminate those that did not.

Feedback should include key questions, such as:

- Is the product usable?
- Is it timely?
- Was it in fact used?
- How was it used?
- Did the product meet expectations? If not, why not?
- What next?

The answers to these questions will lead to refined production, greater use of intelligence by decision makers, and further feedback sessions. Thus, production of intelligence generates more requirements in this iterative process.

MPS 25 – Remote Assurance

Intent

The Company is in an advantageous position with respect to Diamond Intelligence in that the Government of Botswana has a very strong Criminal Intelligence capability due to the Strategic importance of the Diamond Industry for Botswana. It is important that The Company's Security Team plays a supportive role to this Government capability and that is then the intent of this MPS.

Required Actions

25.10 The Company should have an internal capability to support the initiatives of Government Diamond Intelligence activities

25.11 Formal and regular interactions with Government and Local Authorities should be maintained and record kept of all interactions.

25.12 Formal meetings should be held at least once per quarter with Government Intelligence structures to discuss matters of mutual interest.

25.13 The MD The Company should be briefed in detail on the discussions during these meetings.

25.14 Regular interactions (at least monthly) should be maintained with other diamond operations in the region and a formal documented meeting should be held at least once per quarter.

25.15 The Risk Manager (Security) should attend all the meetings with respect to intelligence and investigations and brief the General Manager on a need-to-know basis.

25.16 Persons assigned to the intelligence support activities should clearly understand that they do not have certain jurisdictions outside of the operational area of the mine and should therefor be careful to act within the legal framework of the country.

25.17 The security incident reporting system should be analysed on a continuous basis to determine suspicious activities of persons. Specific attention should be directed to persons that repeatedly contravene operational procedures.

25.18 Other systems like the access control system, seal management, cctv, process maintenance etc should be cross referenced during this analysis these investigations.

Guidance:

What is Intelligence?

Intelligence is the umbrella term referring to the range of activities – from planning and information collection to analysis and dissemination – aimed at maintaining or enhancing relative security by providing forewarning of threats or potential threats in a manner that allows for the timely implementation of a preventive policy or strategy.[20]

The term "intelligence" often conjures the practice of espionage, thoughts of illicit or covert activities. This is not the context in which the term "intelligence" it is being utilized or referred to.

The term "intelligence" here should be considered as the sum total of two very distinct actions occurring in harmony with each other.

Information + Analysis = Intelligence

"Though often used interchangeably and incorrectly, there is a difference between information and intelligence. Unprocessed information helps raise awareness and understanding. When this information is analyzed and evaluated, it becomes intelligence. Intelligence provides situational

[20] Peter Gill & Mark Phythian - Intelligence in an Insecure World – Polity Press 2006

understanding that enables better decision-making. Information plus analysis equal intelligence. [21] "

Being Intelligence Led is a process that will provide for the Security Department at the operational level to achieve maximum effectiveness. It provides for an encompassing organizational approach leveraging on numerous streams of information allowing for timely and tactical decision-making and paves the road for future strategic efforts to maximize resiliency.

Understanding the Intelligence Cycle[22]

In efforts to achieve internalized resilience, one need to fully understand the process, which must be followed. The process utilized to achieve this goal is referred to as the Intelligence Cycle. These very basic steps must be adhered to which will provide our Security Efforts to be truly and effectively Intelligence Led.

The Intelligence Cycle has four Key Processes

5. Requirements & Planning
6. Collection
7. Exploitation & Analysis
8. Dissemination

Requirements & Planning

As with any investigation, a starting point is required. The basic questions that always must be asked and determined are referred to as "W-5" — Who? What? When? Where? Why? (…And potentially the most important and evasive question to be answered is How?)

The answers to the specific questions will also be utilized as the starting points for identification of your respective intelligence needs into requirements of your respective Security Unit. These specific points will formulate the specific framework for decision makers who will determine and establish the Essential Elements of Information, and the planners and the intelligence staff. Typically, an individual is assigned as the Intelligence Resource of the Security Team and will be responsible for generating the Intelligence Requirements specific to the Business Unit, driving the production process.

Once the Intelligence Requirement is defined, spawned from internal or external vulnerabilities, potential threats or pressures, is then transferred into a Collection Plan. A specific individual quality trait of the Security Intelligence Resource is to identify the type of person will determine whether the intelligence produced is responsive to the user's requirements. Where intelligence is playing an increasingly important role, the focus is maintained primarily on the reduction of risk through the identification of potential vulnerabilities Government intelligence requirements are expressed in terms of foreign threats to national or international security. In the business arena, where intelligence is playing an increasingly important role, requirements will generally be expressed in terms relating to individuals or groups involved within the illicit diamond trade.

Planning encompasses the entire intelligence process, beginning with the threat assessment phase and culminates with the delivery of the finished intelligence products. Plans are generated that are responsive to known or anticipated intelligence requirements.

[21] US Department of Justice – Global Justice Information Sharing Initiative "Navigating your Agency's Path to Intelligence Led Policing" April 2009
[22] The Intelligence Cycle White Paper – Bob Foose Techwriter.net 2006

Collection

The collection requirement specifies exactly how the intelligence service will go about acquiring the intelligence information the customer needs. It is normal for several players in the intelligence community to be involved in formulating collection requirements. Collection requirements may be managed by a group of specialists acting as liaisons between users and the collection resources. In non-government organizations collection management may be relegated to one person or team within an intelligence or operational security unit.

Collection requirements management entails much more than simple administrative duties. It requires analytic skill to evaluate how well the user has expressed the need; whether the collection assets are able to obtain the identified information, and how the collected information reaches the intelligence analyst.

Information from open sources are often a valuable collection resource in the business environment, including corporate publications, advertising, newspapers, periodicals, academic journals, foreign and domestic broadcasts, official documents and other published material. Analysts should not participate in any unlawful covert and or clandestine resources while performing this important collection task.

Exploitation & Analysis

Exploitation and analysis involve a series of mental operations various types of collected information or data with close examination of related items of information to determine the extent to which they confirm, supplement, or contradict each other, and thus establish probabilities, relationships, and conclusions. Analysts in all operational programs use their knowledge of regional, national, and global trends to assess the quality of all types of information gathered, and organize it into a responsive, useful intelligence product.

The purpose of intelligence analysis is to reveal to a specific decision maker the underlying significance of selected target information. Frequently intelligence analysis involves estimating one possible outcome, given the many possibilities in a particular scenario. This function is not prediction although in some cases it might be seen as such. The analysis typically can involve forecasting, which requires the analyst to make explicit statements about the degree of confidence held in a certain set of judgments. There are different levels of analysis associated with the production process, usually with results in corresponding levels of conclusions.

In intelligence analysis, the analyst typically does not have direct access to the observable subject, but, instead, gathers information from a variety of sources then proceeds to generating tentative explanations for a subject activity, event, or phenomenon. Each hypothesis is examined for plausibility and compared against the acquired information, in a continual process toward reaching a conclusion. Often the intelligence analyst tests several hypotheses at the same time, generating potential scenarios, and testing each using a rigorous mental processes, subject domain knowledge, experience, and a variety of other associated background “skills.”

The successful intelligence analyst brings to the discipline:

- Certain requisite knowledges and abilities,
- Has necessary aptitude for specialized training,
- Can perform the specific tasks associated with the job, and
- Exhibits personality traits compatible with intelligence analysis work.

This profile is valid in any setting of intelligence activity.

The previously described steps of the cycle are necessary precursors to intelligence production, but it is only in this step that functionality of the whole process is achieved. Production results in the creation of intelligence, that is, value-added actionable information responsive to the user's needs. In practical terms, production refers to the creation, in any medium, of either interim or finished briefings or reports for use by other analysts, decision makers, or policy officials. The general production principles apply to both government and private sector intelligence operations.

Reporting and Dissemination

The production of intelligence is without relative value unless it is timely and reaches the prospective users in a form that allows exploitation of the intelligence. The business environment today is extraordinarily dynamic, with the result that information and intelligence is time sensitive, at highest value at the time of acquisition and depreciates rapidly from that moment. Actionable intelligence is perishable, although it may serve well as historical information too. The key, then, is expedited production and dissemination for action.

The intelligence process does not end with delivering the product to the customer. Instead, it continues in with dialogue between producer and user. If the product is to be useful, dissemination involves feedback. Intelligence producers need feedback from end-users.

They need to know what is useful and not useful to meet the intelligence requirements. Then producers can modify their practices to further develop those activities that served the user well and improve or eliminate those that did not.

Feedback should include key questions, such as:

- Is the product usable?
- Is it timely?
- Was it in fact used?
- How was it used?
- Did the product meet expectations? If not, why not?
- What next?

The answers to these questions will lead to refined production, greater use of intelligence by decision makers, and further feedback sessions. Thus, production of intelligence generates more requirements in this iterative process.