GROUP SECURITY STANDARD

RISK MANAGEMENT

NO. 2

	DESIGNATION	NAME	SIGNATURE	DATE
REVIEWED BY:	GSM: TECHNOLOGY	RUDI LOUW	ORIGINAL SIGNED	15/12/2018
AUTHORISED BY:	VP: GROUP SECURITY & HUMAN RIGHTS	BRIAN GONSALVES	ORIGINAL SIGNED	15/12/2018

DESCRIPTION OF CHANGE:

Version 1.1

Revised & Reviewed June 2012

November 2014 - Inclusion of Bow Tie methodology (4.1 & 4.3.3); Elaboration of Threat Assessment (4.2); Standard use of Risk Matrix (4.3); Inclusion of Strategic Security Risk Themes & Top-level Security Risk Titles (4.5.3)

December 2018 – Critical Control definition and control effectiveness rating (4.3.3)

INDEX

1. INTRODUCTION

AngloGold Ashanti's Chief Executive Officer is accountable for the design, implementation and monitoring of the AngloGold Ashanti group risk management plan, enactment of policy as set by the Board of Directors and provide assurance in this regard. This standard documents the minimum standards for the integration of the Security discipline with group risk management methodology.

2. PURPOSE

As stated within AGA Risk Management Policy and Standards, Risk management is a central part of group strategic management and is the system whereby the risks associated with group activities are methodically addressed with the goal of achieving sustained benefit. Risk management should increase the probability of success, and reduce both the failure potential and the uncertainty associated with achieving the group's overall objectives. Security Risk Management's main objective is to support this strategy by:

- Avoiding or reducing adverse threats to business objectives to an acceptable level and exploiting beneficial opportunities to add sustained value to all group activities.
- Provide timely risk situation information and appropriate risk responses for evaluation of business strategy to assist with meeting business objectives.
- Reduce future operational performance uncertainty by minimizing surprises and associated costs and losses.
- Develop and implement a best practice Security risk management system that is owned and championed at all levels of the organization.
- Monitor and report on group and industry risk trends and outcomes and ensure appropriate Board and the Executive Committee reporting and briefing.
- Ensure that Security risk management forms an integral part of normal business practices and engenders a culture of risk awareness.

3. ACCOUNTABILITY

This standard applies to all company managed exploration and operational sites in AngloGold Ashanti.

The Security Manager is responsible for ensuring compliance to this standard and that the appropriate protocols and control measures are implemented to ensure effective communication.

4. MINIMUM STANDARDS

4.1 AGA Security Risk Management Methodology

Is characterized as the overall process of risk identification, risk quantification and risk evaluation in order to identify potential opportunities or minimise loss, and manage those risks to an acceptable level across the business. Risk management is defined as an ongoing cycle. Based on our approach to Security Risk Management, once risks have been properly identified, assessed and ranked, operations have four options to manage such risks:

- Tolerate
- Terminate
- Treat
- Transfer

By applying the following risk management principles:

- Modify likelihood: Security Management
- Modify impact: Crisis Management Process (Emergency plans, etc)

The bowtie methodology is used for risk assessment, risk management and (very important) risk communication. The method is designed to give a better overview of the situation in which certain risks are present; to help people understand the relationship between the risks and organizational events.

4.2 Threat Assessment

AngloGold Ashanti Global Security defines Threat assessment as the process of identifying and evaluating the *sources* of potential risk. To quantify the sources of security risks, we examine these sources, its characteristics and more specifically their Capability and their Intentions towards company interests (People, Assets and Reputation = PAR)

Threat assessment should consider the following:

- Actors: criminals, communities, employees, gangs, militia, etc.
- *Security Forces:* could be either/or, both, private and public security.
- *Density:* how is the group organized, dispersed, or typically operates on our tenement.
- *Distance:* geographical location (in KMs and cardinal direction) from our project, people, infrastructure or assets.
- *Reaction Time:* Travel time (minutes, hours, days) to arrive at our location (via mode - foot or vehicle).
- *Threat Types:* attack, kidnapping, theft, assault, extortion, etc.
- *Capability*: number of men, type arms, logistics, organization, power projection, etc. (necessary to execute actions, in our area of interest).
- *Intentions*: history, incidents, statistics - evaluating future likelihood to conduct actions

Threat = Capability + Intentions (T= C + I)

Once a detailed assessment has been completed, all findings should be captured within the Global Security Information Management System (GSIMS) Threat Assessment module of the particular site, in order to visualize the site's security threats.

4.3 General Security Risk Assessment

Risk Assessment is the process by which risks are identified and the potential impact of those risks determined according to AGA's risk management matrix.

Use of the matrix can be summarized as:

- Determine what the probability of the event (the thing that goes wrong) could be – the probability is the likelihood that the thing could go wrong.
- Then evaluate the consequence(s) and for the event establish the maximum reasonable consequences that may occur.
- Then for each of those consequences look at an exposure probability - that means the likelihood of that consequence occurring when that event occurs.

A unique risk title is created for each identified risk that is succinct and describes the root cause clearly, but importantly must be aligned to the Global Security high-level risk titles. Risk titles are owned by the operational and project risk owners and can be added and modified by the appropriate risk champions.

4.3.1 AGA Risk Classification and Response

According to AGA's Risk Matrix, risk shall be classified, reported, monitored and will operational generate response as follows:

Classification:	Response:	Report to:	Monitoring:	Risk Planning:
(31-36)	Immediate and urgent action	VII, VI, ERO, RO & Board	Weekly	Business continuity/ contingency and emergency plans mandatory
(25-30)	Proactive management	V, ERO, RO & Board	Monthly	
(16-24)	Active management	IV & RO	Quarterly	Business continuity/ contingency and emergency plans advisory
(9-15)	Manage routinely	III & RC	Routinely	
(1-8)				

4.3.2 Gold Process Risk Assessment and Risk Mapping

A detailed risk assessment should be done on the complete gold process at every site's plant and refinery flow by taking into account the following factors.

- Identification of all areas where gold bearing material and gold in solution is available and accessible.
- Assess the gold value g/t at each identified area.
- Assess the ease of liberating the gold.
- Identify the number of people who could possibly obtain access (Authorized or unauthorized) and then a percentage of that number who could possible steal gold bearing material.

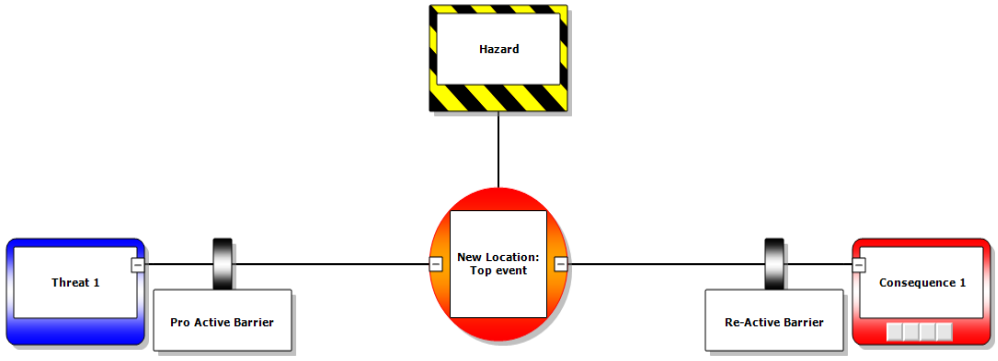
Once a detailed assessment has been completed, all findings should be superimposed with a flow map of the particular site in order to visualize the site's security risk profile.

4.3.3 Bow Tie Methodology

Bow Tie tool and methodology can be used to establish relationship between, hazards, top events, threats and consequences.

The hazard is part of normal business but with the potential to cause harm, can be released by:

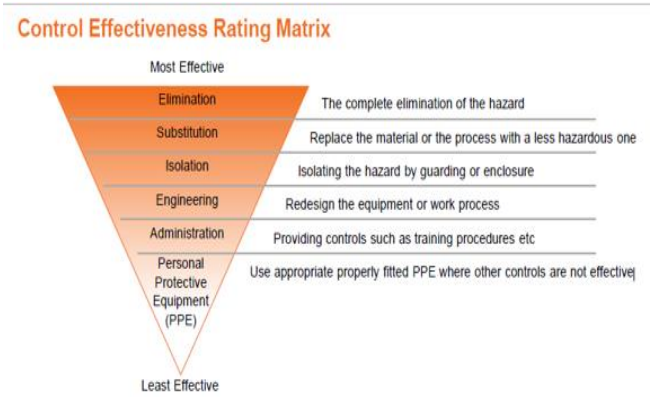
- A top event, not catastrophic yet but the first event in a chain of unwanted events.
- The top event can be caused by threats (sufficient or necessary causes).
- The top event has the potential to lead to unwanted consequences.
- (Proactive) barriers are measures taken to prevent threats from resulting into the top event.
- (Reactive) barriers are measures taken to prevent that the top event leads to unwanted consequences.
- An escalation factor is a condition that defeats or reduces the effectiveness of a barrier.

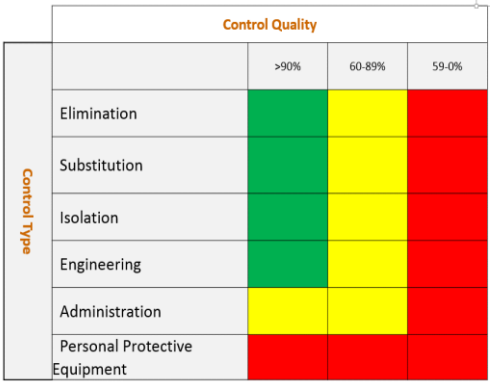


Critical controls are those barriers, which if compromised will lead to the development of the top event or significantly increase the consequences and will include:

- Those controls if compromised to any extent will render all other controls in the same pathway or multiple pathways ineffective realizing the top event.
- Those controls which independently will prevent the top event to realize, even on failure of other controls in the same or multiple pathways.

Control Effectiveness Rating is a method for subjectively establishing the level of effectiveness of an individual control considering its type using the Hierarchy of Control, as well as its quality based on how often it will work when required.





4.4 Vulnerability Checks

Once risks have been identified and assessed and corresponding measures and plans have been implemented, it becomes necessary to verify both compliance and effectiveness of the measures. To this effect, security managers should implement a coherent and documented Vulnerability Check system e.g. random unannounced test on security employees/posts and/or systems. Some examples of these tests are:

- Vehicle/Personnel Searches (using people and/or technology) – are procedures followed and theft of property detected?
- Perimeter Protection – is an “intrusion” detected and does the system automatically initiate the required response.
- Rapid Response Units – is the response time adequate to mitigate the risk.
- CCTV system configuration – does the surveillance management system alert control room operators in the event of unauthorised movement at high risk areas?

These checks will be recorded, and their outcome will support security management in cases were additional training or procedural changes may be necessary.

4.5 Integration with AGA AuRisk

4.5.1 Operational Risk Owner

As risks are owned by the operational or project risk owners, the risks may not be altered by others including the risk management process owner (other than for administrative purposes) and functional risk owners.

The (operation/ project) Security risk owner shall:

- Have primary accountability for implementing, maintaining and embedding the risk management system and process within his/ her area.
- Promote risk awareness within his/ her area.
- Set risk management objectives for his/ her area.
- Incorporate into business plans details of the provision of resources to mitigate peak threats to acceptable levels and harness key opportunities.
- Report Risk Rising to relevant management, risk champion and functional risk owner.

4.5.2 Functional Risk Owner

Functional risk owners are to review the risk titles per operation and project to confirm that the risks in their area of ownership are appropriate, adequate and correctly evaluated. Where there is disagreement, the functional risk owner is to contact the operational/ project owner or his champion and recommend adjustment or external review. Should agreement not be achieved, the functional risk owner is to escalate the issue to the relevant executive risk owner for resolution.

Prior to Board reporting, functional risk owners are required to confirm that they have reviewed the risks contained with the applicable sub-categories for all operations and projects.

Agreement on the evaluation of the High-Level Top 14 risks must be obtained.

4.5.3 Security Risk Category and Sub-Categories in AuRisk

The **categories** provide a classification system for the sorting, reporting and management of risks and are used within *AuRisk* and for Board reporting. Categories are seen as the **strategic security risk themes.**

Sub-Categories are defined per main category to encourage a systematic consideration and naming of risks, which is important for the identification of risk aggregation. Sub-categories are seen as the Global Security high **level security risk titles**.

Risk sub-categories are defined and owned by the functional risk owners and are to be modified as necessary in consultation with the risk management process owner.

Risks in the Security risk management category relate to acts or practices that affect the security of assets or personnel. Also included are security acts or omissions that have the potential to impact group reputation. See table below for reference:

5. REVIEW

The standard will be reviewed every two years (Biennial).

6. COMMUNICATION

The standard will be communicated to the Security Manager at each operation for appropriate distribution. Copies will be provided to the relevant EVP'S, SVP'S, VP'S and GM/MD'S as required.

7. REFERENCES

7.1 AGA Group Risk Management Policy

7.2 AGA Group Risk Management Standard

7.3 AGA Risk owner and champion definition

7.4 AGA Risk Assessment Matrix

7.5 Group Security High Level Risk Package