IMAS 07.14

First Edition
February 2019

Risk Management in Mine Action

Director,
United Nations Mine Action Service (UNMAS)
1 United Nations Plaza
New York, NY 10017
USA

Email: mineaction@un.org
Telephone: +1 (212) 963 0691
Website: www.mineactionstandards.org

Warning

This document is current with effect from the date shown on the cover page. As the International Mine Action Standards (IMAS) are subject to regular review and revision, users should consult the IMAS project website in order to verify its status at (http://www.mineactionstandards.org/, or through the UNMAS website at http://www.mineaction.org).

Copyright notice

Director
United Nations Mine Action Service (UNMAS)
1 United Nations Plaza New York,
NY 10017 USA
E-mail: mineaction@un.org
Telephone:+1 (212) 963 0691
Website: www.mineactionstandards.org

Contents

Foreword

International standards for humanitarian demining programmes were first proposed by working groups at an international technical conference in Denmark, in July 1996. Criteria were prescribed for all aspects of demining, standards were recommended and a new universal definition of 'clearance' was agreed. In late 1996, the principles proposed in Denmark were developed by a UN-led working group and the International Standards for Humanitarian Mine Clearance Operations were developed. A first edition was issued by the UN Mine Action Service (UNMAS) in March 1997.

The scope of these original standards has since been expanded to include the other components of mine action and to reflect changes to operational procedures, practices and norms. The standards were re-developed and renamed as International Mine Action Standards (IMAS) with the first edition produced in October 2001.

The United Nations has a general responsibility for enabling and encouraging the effective management of mine action programmes, including the development and maintenance of standards. UNMAS, therefore, is the office within the United Nations responsible for the development and maintenance of IMAS. IMAS are produced with the assistance of the Geneva International Centre for Humanitarian Demining.

The work of preparing, reviewing and revising IMAS is conducted by technical committees, with the support of international, governmental and non-governmental organisations. The latest version of each standard, together with information on the work of the technical committees, can be found at http://www.mineactionstandards.org/. Individual IMAS are reviewed at least every three years to reflect developing mine action norms and practices and to incorporate changes to international regulations and requirements.

Introduction

Managing risk is fundamental to every aspect of mine action. Not just in the most obvious ways of keeping staff safe and ensuring that released land is safe for end-users, but in relation to every decision that mine action managers and other staff take: Which projects and programmes to support, who to hire, how to train people, what equipment to buy, how to maintain relationships with stakeholders, which tasks to prioritise, and how to manage quality and environmental aspects of mine action operations. A starting point for effective risk management is awareness of its importance and constant association with everything that mine action managers do every day. This standard seeks both to raise awareness and equip mine action managers with the tools they need to identify, assess, control and review risk within their many different areas of responsibility. Annex B to this standard includes guidance on the use of a range of risk identification, assessment and analysis tools.

In the ISO system, risk is defined as 'the effect of uncertainty on objectives' where there is uncertainty there is risk. Conversely, where there is knowledge there is confidence, and uncertainty and risk are reduced. The definition indicates the most important way to reduce risk - through the collection, analysis and sharing of information. Good information management is fundamental to effective risk management.

The principles and processes described in this IMAS are applicable to any situation in which mine action managers must take decisions about achieving objectives, satisfying requirements, releasing land and retaining stakeholder confidence. In some specific situations aspects of risk management are dictated by existing documented sources. Of these the most significant relate to the requirements of international treaties – the Anti-Personnel Mine Ban Convention (APMBC), the Convention on Cluster Munitions (CCM) and Protocol V of the Convention on Certain Conventional Weapons (CCW). Questions of tolerability of residual risk are directly addressed in the relevant text and provide a clear basis upon which mine action managers must work. The treaties form part of the surrounding environment that mine action managers must consider when establishing effective risk management systems.

Risk management, like most other management systems, is not in itself complicated or difficult to do (although in larger organisations a risk management system may become widespread and demand a high level of management attention). It relies upon the repeated application of simple principles and processes, consistently and comprehensively, at every level within an organisation. Other management aspects within the IMAS system, including quality, safety, occupational health, environmental management and information management all represent the application of basic risk management principles and processes. Effective and efficient managers, whatever their area of responsibility, will also be effective and efficient risk managers.

The IMAS system provides a basis for the development of national mine action standards (NMAS), but they may also be used as standalone standards in their own right and provide input to help mine action organisations develop their own policies, processes and procedures. The guidance provided in this standard is applicable to all mine action organisations, at every level.

Prevailing circumstances and conditions determine both the scope and speed of response that any risk management system must exhibit if it is to remain effective. Fast changing circumstances (such as those associated with some situations where improvised explosive devices (IEDs) are present) demand risk management systems that can adapt, update and evolve very quickly. Others may remain adequate for longer periods without the need for substantial changes. In every case a risk management system only remains effective if it is reviewed and updated often enough to ensure that it reflects significant changes in the surrounding circumstances as and when they occur.

This standard aims to provide mine action managers, at every level, with the guidance they need to identify and manage the risks associated with their work and responsibilities. It draws on the guidance provided in ISO 31000 Risk Management – Guidelines adapting them to reflect the nature of the mine action sector.

Risk Management in Mine Action

1 Scope

This standard provides guidelines for the implementation of recognised risk management principles, practice and processes in mine action programmes and organisations.

It is primarily intended for application by national mine action authorities (NMAAs) and national mine action centres (MACs), but its principles remain valid for, and should be used to form the basis of, risk management systems developed and employed by all mine action organisations.

This standard should be used in conjunction with IMAS 07.12 `Quality Management in Mine Action` and IMAS 07.40 `Monitoring of Mine Action Organisations`.

2 References

A list of normative references is given in Annex A. Normative references are documents to which reference is made in this standard and which form part of this standard.

3 Terms, definitions and abbreviations

A complete glossary of the terms, definitions and abbreviations used in the IMAS series is given in IMAS 04.10.

In the IMAS series, the words 'shall', 'should' and 'may' are used to indicate the intended degree of compliance.

a) 'shall' is used to indicate requirements, methods or specifications that are to be applied in order to conform to the standard;

b) 'should' is used to indicate the preferred requirements, methods or specifications; and

c) 'may' is used to indicate a possible method or course of action.

The term 'National Mine Action Authority' (NMAA) refers to the government entity, often an interministerial committee, in an EO-affected country charged with the responsibility for broad strategic, policy and regulatory decisions related to mine action.

Note: In the absence of an NMAA, it may be necessary and appropriate for the UN, or some other body, to assume some or all of the responsibilities of an NMAA.

A mine action organisation is “any organisation (government, military, commercial or NGO/civil society) responsible for implementing mine action projects or tasks. The mine action organisation may be a prime contractor, subcontractor, consultant or agent.” (IMAS 04.10).

Risk is “the effect of uncertainty on objectives” (ISO 31000:2018). Risk may be expressed in terms of risk sources, potential events, their consequences and their likelihood.

In general risk management, residual risk is “the risk remaining after risk treatment” (ISO 27001:2013)

In technical mine action, residual risk is “the risk remaining following the application of all reasonable effort to identify, define, and remove all presence and suspicion of explosive ordnance through non-technical survey, technical survey and/or clearance.” (IMAS 04.10).

Context is “the combination of internal and external issues that can have an effect on an organisation’s approach to developing and achieving its objectives” (ISO 9000:2015).

Internal context is 'the parameters and factors that fall within the internal decision-making authority and ability of an organisation and that can influence the establishment and achievement of objectives, including the organisation's internal stakeholders, approach to governance, contractual relationships, capabilities, culture, and standards. Governance includes the organisation's structure, policies, objectives, roles, accountabilities, decision-making processes, and capabilities including its knowledge and human, technological, capital, and systemic resources'.

Note: guidance on understanding and defining an organisation's internal context is provided in section 7.1.1 of this standard.

External context is 'the local, national, and international parameters and factors, that influence the establishment and achievement of objectives and that fall outside the exclusive decision-making authority of an organisation, including external stakeholders, their values, perceptions and relationships, as well as key drivers and important trends within the social, cultural, political, professional, legal, regulatory, technological, economic, natural, and competitive environment'.

Note: guidance on understanding and defining an organisation's external context is provided in section 7.1.1 of this standard.

All reasonable effort "describes what is considered a minimum acceptable level of effort to identify and document contaminated areas or to remove the presence or suspicion of explosive ordnance. All reasonable effort has been applied when the commitment of additional resources is considered to be unreasonable in relation to the results expected" (IMAS 04.10).

Risk treatment is "the selection and implementation of options for addressing risk". Risk treatment in mine action may also be referred to as "risk mitigation' or 'risk reduction".

A risk control is "a measure that maintains and/or modifies risk" (ISO 31000:2018). In mine action a risk control is normally one that reduces/mitigates risk.

Risk evaluation is the "process based on risk analysis to determine whether the tolerable risk has been achieved" (IMAS 04.10).

Improvement is "activity to enhance performance" (ISO 9000:2015).

A stakeholder is a "person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity" (ISO 31000:2018).

4 Purpose

The purpose of risk management in mine action is to identify, assess, control and review risk wherever it may arise, such that mine action programmes, projects and activities are safe, efficient and effective in achieving their objectives.

5 Principles & cross-cutting issues

5.1 Importance of Risk Management Systems

Risk management is fundamental in all mine action programmes. Among other aspects, it helps managers and other staff to ensure:

- Better identification of opportunities and threats associated with organisational initiatives;
- Compliance with relevant legislation;

- Improved capability to negotiate/discuss standards;
- Greater openness and transparency in decision-making and ongoing management;
- improved loss control, reduced loss/incident damage and cost of risk;
- Control of commercial insurance premiums;
- Learning and promulgating lessons from both successes and failures;
- Avoidance of costly surprises through early identification and management of risk;
- better programme governance and organisational protection;
- Improved stakeholder confidence and the potential for enhanced fundraising;
- A more rigorous basis for planning through structured consideration of key risks;
- More effective allocation and efficient use of resources; and
- Improved communication and consultation, both internally and externally.

5.2 Leadership and commitment

All management systems rely upon clear evidence of support and commitment from senior managers. Specific responsibilities of National Mine Action Authorities (NMAAs), Mine Action Centres (MACs), mine action organisations, donors and other relevant stakeholders are set out in Section 8 of this standard.

5.3 Appropriate, comprehensive and inclusive system

The risk management system should:

- Be appropriate to the mine action context, activities and expectations of stakeholders;
- Reflect commitments to meet obligations under applicable international treaties;
- Be comprehensive in addressing all types of risk relevant to the mine action programme, project or organisation and its context; and
- Ensure timely and appropriate involvement of stakeholders, including consideration of their knowledge, views and perceptions.

5.4 Communication & consultation

The risk management system should:

- Draw on the knowledge, expertise and experience of stakeholders as well as databases and other information resources, to assist in the identification, analysis and evaluation of risk and in the establishment of risk criteria; and
- Communicate to relevant stakeholders the information they need in order to be aware of, and manage effectively, risks relating to their own activities and responsibilities.

Establishing effective, timely, user-friendly, easily accessible mechanisms for the sharing of information relating to the management of risk amongst mine action stakeholders is an essential aspect of effective risk management in mine action. Mine action authorities, managers and decision-makers should take all reasonable steps, in cooperation with mine action information managers, towards the establishment of such mechanisms.

5.5 Dynamic and responsive

Risk management systems should be able to improve, adjust and respond at a rate appropriate to changes in the external and internal context. In some situations of emergency or rapidly developing circumstances, mine action risk management systems may need to function quickly and often, completing the cycle of risk identification, assessment, treatment and review at short intervals. Risk management is often the first element of any management system to 'hit the ground' in new and challenging circumstances. To be reliable, mine action risk management systems must be able to cope with such demands, providing a foundation on which all other practical, administrative, logistic and strategic decision-making can be based.

5.6 Integration

Risk management and information management are integral to all management systems. While they have their own intrinsic cyclical management systems, they provide the fundamental basis upon which all other management systems are founded. The most significant examples within mine action include strategic management, results-based management (RBM), quality management (QM), environmental management (EM) and occupational health and safety management (OH&SM). All constitute risk management, supported by good information management.

Mine action Standard Operating Procedures (SOPs), as well as IMAS and NMAS, all help manage risks associated with how mine action is directed, defined, implemented, monitored and improved in order to deliver reliable results to stakeholders.

Risk management provides important inputs into those other systems and in turn relies upon information received from those systems to ensure that it remains relevant, up-to-date and effective. Risk management is only fully effective when it is properly integrated into all aspects of mine action management systems.

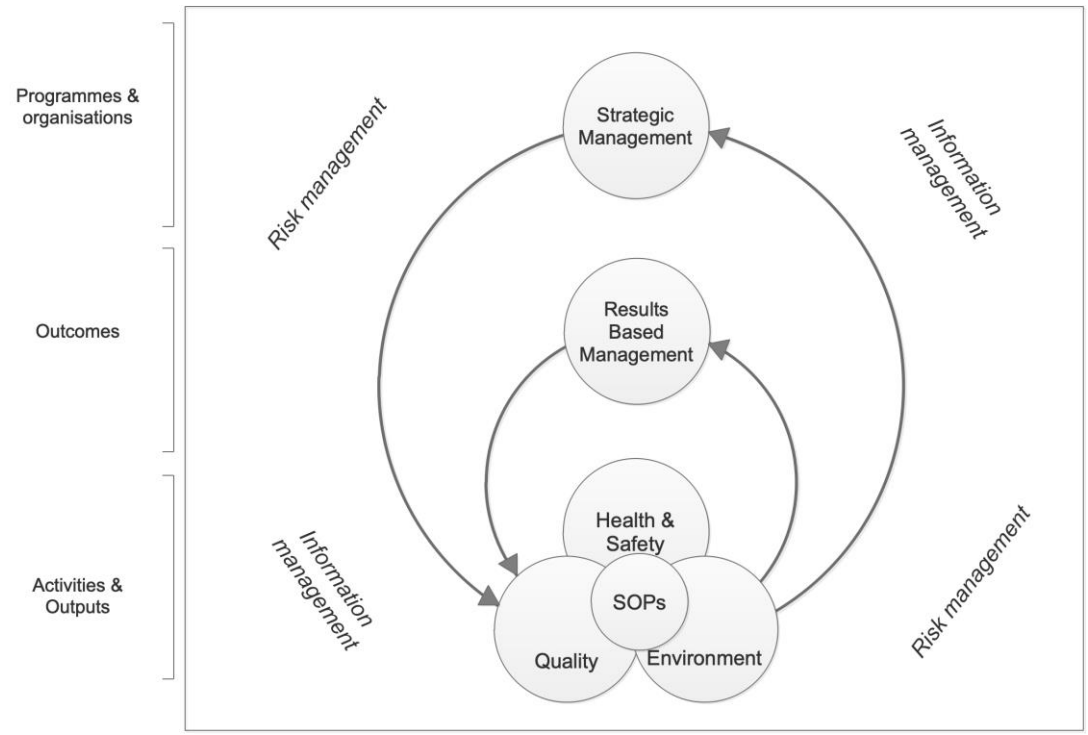


Figure 1: interaction of management systems and procedures at different levels within the overall framework of risk and information management.

5.7 Information management

Up-to-date and comprehensive information management is essential to effective risk management. The timely provision of relevant Information comprises the primary means to reduce uncertainty and so to reduce risk.

The structure and content of mine action information management systems should be informed by the needs of risk management including the collection, reporting and quality management of relevant data and the analysis and dissemination of findings relevant to risk management by stakeholders.

5.8 Human factors

The human brain is not well equipped to make objective sense of large volumes of experiential data. Instinct, habit and emotion all influence, and in most cases reduce, the analytical capabilities of the brain. As a result, the reality of risk is often very different from the way it is perceived by individuals and groups of people. Risk managers should be aware of, and make appropriate allowance for, the limitations associated with human factors in understanding and responding to risk. A range of cognitive biases have been identified and studied by academic and industrial researchers. Of particular significance to mine action risk managers are:

- **Availability heuristic** - the tendency to think that examples of things that come most readily to mind (because they are unusual, interesting, exciting, frightening, etc.) are more representative than is actually the case;
- **Anchoring** - the tendency to rely too heavily on a past reference or on one piece of information when making decisions;
- **Confirmation bias** - the tendency to interpret information in a way that confirms preconceptions;
- **Bandwagon effect -** the tendency to do or believe things because many other people do or believe the same; and
- **Unconscious bias** - the unconscious attribution of particular qualities to a member of a certain social group.

Other cognitive biases may be relevant in some circumstances. To reduce the effects of cognitive biases, quantitative data, where available, and structured qualitative systems should always be used in preference to reliance upon purely subjective human perceptions when assessing and managing risk in mine action.

5.9 Age, gender and diversity

The likelihood and consequences of different risks may vary greatly between different age and gender groups and persons with disabilities, as well as between different ethnic, cultural and religious groups. Risk managers should recognise and take into account such differences when identifying, analysing, evaluating and treating risks.

Sex and age disaggregated data (SADD) should be collected and used to support the effective identification, assessment, analysis and treatment of risk.

Risk managers should ensure that women, girls, boys and men are appropriately included in consultation and participation processes and procedures within mine action risk management systems.

5.10 Continual improvement

Mine action risk management systems should be subject to continual improvement in accordance with IMAS 07.12 `Quality Management in Mine Action`.

5.11 Residual risk, all reasonable effort and ALARP

The treatment of risk (meaning those actions taken to reduce, mitigate or otherwise modify risk) rarely removes risk entirely. In most situations some risk remains after treatment. Wearing a seatbelt does not reduce the risks associated with a road traffic accident to zero, but it does significantly reduce those risks. Agreeing a currency exchange rate in advance with a bank does not eliminate the risk associated with market fluctuations, but it does ensure they remain within predictable limits. In the academic, scientific, governmental and industrial discipline of risk management, as described in the ISO system, the 'risk that remains after treatment' is defined as the 'residual risk'.

Within the land release process (as described in IMAS 07.11), 'residual risk' is defined specifically as 'the risk remaining following the application of all reasonable effort to identify, define, and remove all presence and suspicion of explosive ordnance through non-technical survey, technical survey and/or clearance'. The IMAS definition is wholly consistent with the ISO definition. The IMAS definition should always be used in relation to land release processes, while the ISO definition is applicable, and should be used, whenever describing and managing risks associated with non-land release aspects of mine action projects and programmes.

If residual risk is not tolerable to stakeholders then further treatment should be identified, implemented and monitored in accordance with Section 7 of this standard.

In terms of safety management, the term ALARP (as low as reasonably practicable) may be used. Application of 'all reasonable effort' is consistent with the achievement of an ALARP level of residual risk in released land.

6 Risk management system

The scope and form of mine action risk management systems should reflect the circumstances and conditions within which mine action operations are undertaken and the size and complexity of the mine action organisation. As a minimum, any mine action risk management system should include:

- A risk register, including risk treatment measures;
- A systematic risk review process;
- Adequate training in implementation and maintenance of the risk management system;
- A register of accidents, incidents, near misses, nonconformities and other risk-related issues and events, including lessons learnt; and
- The maintenance and dissemination of indicators relevant to the risk register (using SADD wherever feasible and appropriate).

Documentation, including policies, procedures and records should be developed to a level appropriate to the scope and context of the risk management system, and as necessary to ensure that mine action risks remain at a tolerable level.

7 Risk management process

Risk management is a cyclical process. Repeated iterations of the process:

- Ensure that the risk management system remains up-to-date and reflects changes in the internal and external context; and
- Support continual improvement of the risk management system.

Key elements of the risk management process (in Figure 2) are:

- Understanding the context within which mine action operations take place. Determining the scope of risk management activity, and establishing risk criteria to support appropriate and effective decision-making;
- Identifying risks relevant to the achievement of mine action objectives;
- Analysing identified risks to understand and characterise risk, and to establish the level of risk;
- Evaluating risk to determine whether the level of risk is tolerable, or whether risk treatment is necessary;
- Defining and implementing risk treatment to modify risk in such a way that the residual risk remaining after treatment is tolerable; and
- Reviewing risk to ensure that the risk management system remains up-to-date, relevant and effective.

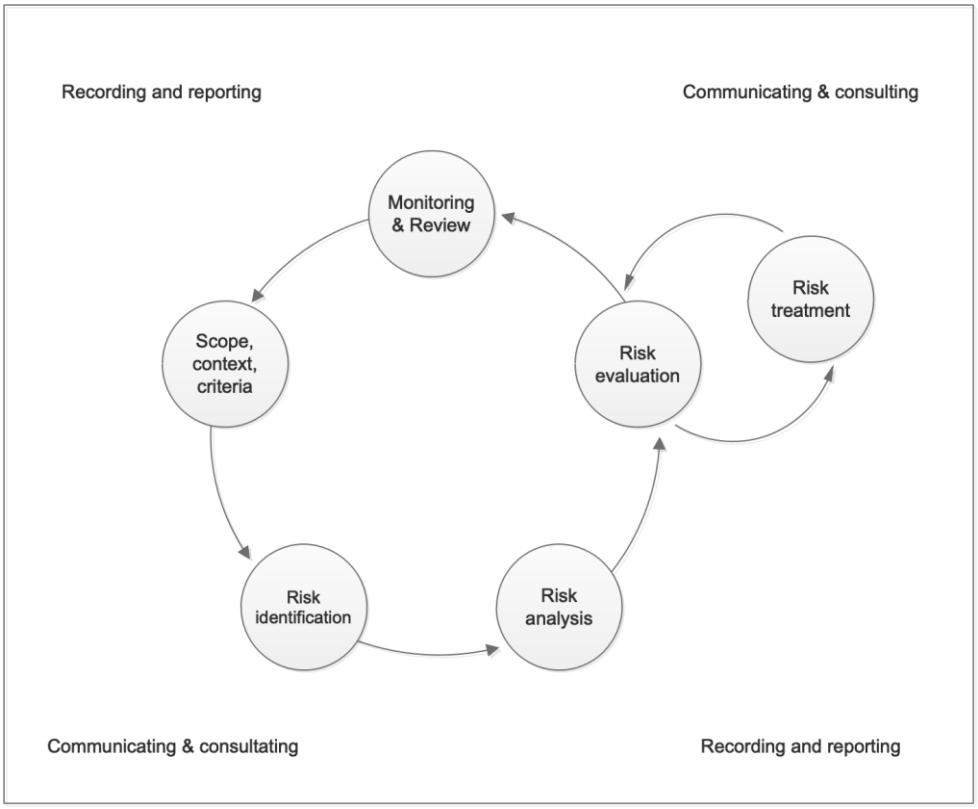


Figure 2: Cycle of risk management in mine action

Surrounding the core elements of risk management cycle are the permanent functions of ‘recording and reporting’ and ‘communicating and consulting’.

7.1 Context, scope and criteria

7.1.1 Understanding the context

The risk management context is the external and internal environment within which a mine action organisation seeks to define and achieve its objectives. In rapidly changing and emergency situations, the ability to understand the context quickly and accurately is likely to be especially important. The early allocation of adequate resources to investigate, analyse and communicate the context is a key responsibility of mine action managers.

Mine action organisations should maintain an up-to-date and accurate description of context adequate to ensure that risks that may impact, positively or negatively, on the achievement of mine action objectives, are identified, assessed and treated effectively and efficiently.[1]

In assessing the external context mine action organisations should consider, but not limit consideration to:

- Social, cultural, political, legal, gender and diversity, regulatory, financial, technological, economic and environmental factors, whether international, national, regional or local;
- Treaty commitments;
- Key drivers and trends relevant to the scope of mine action activities;
- External stakeholder relationships, perceptions, values, needs and expectations;
- Contractual relationships; and
- The complexity of networks and dependencies.

In assessing the internal context mine action organisations should consider, but not limit consideration to:

- The organisation's vision, mission and values;
- Governance, organisational structure, roles and accountabilities;
- Strategy, objectives and policies;
- The organisation's culture;
- The working environment(s);
- Staff composition, including gender and diversity dynamics;
- Standards, guidelines and methodologies adopted by the organisation;
- Capabilities, in terms of resources and knowledge;
- Data, information systems and information flows;
- Relationships with internal stakeholders, including their perceptions and values;
- Contractual relationships and commitments; and
- Interdependencies and interconnections.

[1] A risk that has the potential to yield a positive impact may also be termed an opportunity.

In assessing the context, mine action authorities and managers should make use of recognised tools and techniques including, but not limited to:

- Political, economic, social, technical, legal, environmental (PESTLE) analysis;
- Strength, weakness, opportunity, threat (SWOT) analysis;
- The Mine Action Architecture diagram (detailed in Annex B);
- Stakeholder identification and analysis techniques (power/influence grids, 'onion' diagrams, interface analysis, etc.);
- Gender and diversity analysis; and
- Political Economy Analyses.

7.1.2 Scope of risk management

The scope of risk management in mine action shall be determined on the basis of:

- The scope of operational, administrative and management activities implemented by the relevant mine action organisations;
- An up-to-date and accurate analysis of the external context within which the mine action organisation operates;
- An up-to-date and accurate analysis of the internal context of the mine action organisation; and
- The needs, expectations, requirements and preferences of mine action stakeholders.

The scope shall be adequate to encompass all risks that influence (positively or negatively) the ability of the mine action organisation to achieve its objectives.

In determining the scope of risk management, authorities/managers shall take into account the need for connectivity between risk management and other management systems including strategic, information, quality, safety, environmental, and results-based.

7.1.3 Risk criteria

Risk criteria inform decisions about whether a specified level of risk is tolerable or not. Risk criteria in mine action reflect a combination of globally established criteria (such as those relating to compliance with the terms of international treaties) and criteria reflecting the values, policies and objectives of specific mine action programmes, projects and organisations.

Risk criteria may be defined in contracts, memoranda of understanding, standards, accreditation agreements, policies, procedures or other relevant documents. Risk criteria should be established for all categories of risk relevant to the mine action operations. Categories include, but are not limited to:

- Human safety;
- Protection of physical assets;
- Protection and safeguarding of staff and beneficiaries;
- Financial gains and losses;
- Reputational aspects;

- Programme and project management aspects;
- Treaty and legal obligations compliance;
- Stakeholder relationships and perceptions (including 'customers');
- Protection of the environment; and
- Quality management.

Criteria may be established in numerical and/or narrative terms (definitions of critical nonconformity in land release constitute risk criteria for instance). The nature of risk and uncertainty is such that defining criteria in absolute terms may not always be possible. In every case authorities and managers should seek to establish criteria that are as clear, consistent and unambiguous as possible. Criteria should be consistent with the risk analysis methods established in accordance with Section 7.2.2 of this standard and be applicable for the purposes of risk evaluation described in Section 7.2.3 of this standard.

7.2 Identifying and assessing risk

7.2.1 Identifying risk

The purpose of risk identification is to find, recognise and describe risks that may influence, positively as well as negatively, the ability of a mine action programme, project or organisation, to achieve its objectives. Risk identification systems should remain up to date and relevant to the prevailing circumstances and conditions.

Mine action risk managers should make use of recognised methods, tools and techniques, appropriate to the context and scope of their risk management, to support effective and comprehensive risk identification including, but not limited to:

- Political, economic, social, technical, legal, environmental (PESTLE) analysis;
- Strength, weakness, opportunity, threat (SWOT) analysis;
- Brainstorming;
- Interviews;
- Structured 'What if' techniques (SWIFT);
- Focus group discussions;
- Check lists;
- The results of nonconformity, accident, incident and near miss investigations;
- Consequence/likelihood matrix; and
- Trends in key performance indicators (KPIs).

Mine action risks do not only relate to those associated with the location and clearance of hazardous objects. While the safety of members of affected populations and of mine action staff is of the highest priority, the ability of mine action programmes to achieve their objectives depends on a large number of factors ranging from the supply of equipment, through the competence of management and the process of designing programmes and projects, to the availability of a safe/permissive environment in which to carry out work. Effective risk identification in mine action should include consideration of areas of uncertainty and risk in relation to all aspects of the external and internal context within which work is carried out.

7.2.2 Analysing risk

The purpose of risk analysis in mine action is to understand the characteristics and nature of risk including the level of risk. Risk analysis includes consideration of:

- The likelihood (probability) of potential events;
- The nature and magnitude/impact of consequences;
- Interactions between risks and the complexity of those interactions;
- The proximity of risk (how soon it is likely to occur);
- Duration and volatility of risks;
- Site or circumstance specific conditions; and
- The effectiveness of existing risk controls.

Risk analysis may be qualitative, quantitative or semi-quantitative in nature. Mine action risk managers should work closely with mine action information managers to identify opportunities to collect relevant data to support quantitative and statistical analysis of risk wherever it is feasible and efficient to do so.

Mine action risk managers should make use of recognised methods, tools and techniques, appropriate to the context and scope of their risk management, to support effective and comprehensive risk analysis including, but not limited to:

- Levels and trends in key performance indicators (KPIs);
- Consequence/likelihood matrix;
- Structured 'What if' techniques (SWIFT);
- 'Bow tie' analysis; and
- Root cause analysis (RCA).

7.2.3 Evaluating risk

The purpose of risk evaluation is to determine whether risk is at a level that demands risk treatment to reduce/mitigate it to a tolerable residual level. Risk criteria are used to inform decisions about the tolerability of risk.

Establishing the level of risk that is tolerable may reflect a range of inputs including:

- Established historical practice;
- Consultation with relevant stakeholders, including gender and diversity groups;
- Reference to existing legal decisions; and
- Documented requirements in treaties, agreements and other instruments of international and national law.

The result of risk evaluation may be to:

- Take no further action;
- Consider risk treatment options;

- Conduct further risk analysis to understand the risk better;
- Maintain existing risk controls; and/or
- Consider adjusting goals, objectives or other aspects of planned activity.

7.3 Treating risk

The purpose of risk treatment in mine action is to define, implement and confirm the effectiveness of actions to ensure that risk remains at a tolerable level.

7.3.1 Options for treating risk

Options for the treatment of risk include:

- **Avoiding risk** - not undertaking the activity, or avoiding the circumstances, that give rise to the risk;
- **Removing the risk source** - taking action to move, destroy or otherwise separate the risk source from intended activities;
- **Changing the likelihood** - taking action to make it less likely that an event associated with the risk will occur;
- **Changing the consequences** - taking action to reduce the impact of an event on people, assets or perceptions;
- **Sharing the risk** - most commonly in mine action through contractual terms, agreements, teaming arrangements or the purchase of insurance; and/or
- **Accepting the risk** - as one that is already at a tolerable level, or in order to pursue an opportunity.

Not all risk treatment options will be appropriate or feasible in every instance. Risk treatments are not necessarily mutually exclusive. On many occasions a combination of treatment types will be appropriate.

The implementation of a risk treatment may give rise to one or more new risks.[2] Mine action risk managers should consider the potential for the creation of new risks whenever considering the implementation of risk treatment measures.

7.3.2 Residual risk and tolerability

The concept of the 'risk that remains after treatment' (as described in Section 5.11) is an essential component of any effective risk management system.

'Residual risk' as the 'risk that remains after risk treatment' is a definition and concept that is applicable at every level and to any aspect of mine action management. A risk is 'tolerable' when stakeholders are willing to accept that risk, confident that it is worth taking and is properly controlled. As an example, in mine action, stakeholders are content to accept that the risk to a trained and certified deminer conducting clearance operations, working in a well-managed organisation, at a well-managed site, applying proven technical procedures, with a reliable emergency response plan in place, is tolerable. So long as the risk treatment, mitigation or reduction measures are accepted as appropriate, and are properly and

[2] In mine action the most obvious example of this principle is when the clearance of mines/ERW removes a risk source from an affected population, but in doing so creates a new risk for the deminers conducting the clearance work.

effectively implemented, then the risk remaining after that treatment (the 'residual risk') associated with clearance work is tolerable in relation to the benefits that arise from it.

Within the land release process, the concept of residual risk is significant enough to merit its own specific definition in IMAS 04.10, as being "the risk remaining following the application of all reasonable effort to identify, define, and remove all presence and suspicion of explosive ordnance through non-technical survey, technical survey and/or clearance". The implication is that where 'all reasonable effort' has been applied then the residual risk is tolerable. In this case the concept of 'all reasonable effort' provides mine action organisations and institutions with direct guidance on the form of treatment necessary to ensure that the residual risk is tolerable. Accreditation, Quality Assurance (QA) and Quality Control (QC) processes, in accordance with IMAS 07.12, 07.30 and 07.40, are applied in order to confirm that all reasonable effort has been implemented and that the residual risk is tolerable.

The same principle applies to all risk management processes. The level of risk following treatment should be assessed and evaluated against established criteria (as per section 7.1.3). If the level of risk following treatment (the residual risk) is tolerable, then further action is not required. If the residual risk is not tolerable then authorities/managers must consider and implement further treatment options until a tolerable level of residual risk is achieved.

In mine action, aspects relevant to residual risk and tolerability are also addressed in the terms of international treaties including:

- The Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on Their Destruction (APMBC);
- The Convention on Cluster Munitions (CCM);
- The Convention on Certain Conventional Weapons (CCW);
- The Convention on the Rights of Persons with Disabilities (CPRD); and
- Other treaties, conventions and legal instruments that may be applicable depending upon the place, time and nature of the mine action activities.

Decision-making in mine action relies upon application of the principles and processes set out in this standard and shall reflect the requirements of applicable international treaties.

7.4 Risk ownership and liability

The risk owner is a 'person or entity with the accountability and authority to manage a risk' (ISO 27001:2014). Risk ownership in mine action is often implied or assumed on the basis of historical habit and practice, but it may also be defined in:

- Job descriptions;
- Terms of reference;
- Contracts;
- Memoranda of understanding;
- Accreditation agreements;
- Standards and legislation; and
- Other operational and legal documentation.

Responsibility for ensuring that risks are identified, assessed, controlled and reviewed is essential to any effective risk management system. Assessing clarity as to where responsibility lies in relation to the management of risks at different levels and in different

elements within mine action should form part of the assessment of context detailed in Section 7.1.2 of this standard.

Mine action authorities, organisations and managers should ensure that responsibilities and authorisations to manage risk are clearly defined and that monitoring processes confirm that such responsibilities are satisfied.

Liability refers to any legal responsibility, duty or obligation that a country, organisation or individual may have. Liability in relation to an adverse event, such as an accident or the discovery of a missed item in an area, is normally linked to non-compliance with an agreed policy or procedure.

The application of a comprehensive and effective risk management system should ensure that those risks associated with legal liability are maintained at a tolerable level. Guidance on risk and liability aspects relating to land release operations is provided in IMS 07.11.

7.5 Monitoring

Risk management processes should be monitored in accordance with IMAS 07.40 `Monitoring of mine action organisations`. Indicators relevant to the effectiveness of risk management should be established, maintained and monitored. Relevant risk-related indicators may include:

- Incidence, type and severity of accidents and incidents;
- Incidence, type and severity of quality nonconformities;
- Incidence, type and severity of environmental nonconformities and incidents;
- Complaints and other stakeholder feedback;
- Financial value of lost, damaged and stolen assets; and
- Programme/project deviations from plans.

Mine action managers should identify and establish other indicators relevant to the scope and context of the mine action organisation's operations.

7.6 Review

Risk review completes the risk management cycle and provides the primary driver determining how often the risk management cycle functions. In circumstances where internal and external context aspects change often and significantly risk reviews should be carried out more often.

Risk reviews should be conducted:

- In response to significant changes in the context;
- In response to findings in accident and incident investigations, near misses, root cause analysis following nonconformities, etc.; and
- At intervals appropriate to the prevailing circumstances and conditions, but at least annually.

7.7 Recording, reporting and communicating

Mine action risk management systems should include adequate documentation to:

- Define the risk context, scope and criteria;

- Detail risk management procedures; and
- Maintain documented evidence (as per Section 6 of this standard) that the risk management system is effectively implemented.

Documentation may include policies, procedures and records directly associated with the management of risk, as well as reference to relevant documentation from other elements of overall mine action management systems including:

- Quality management;
- Occupational health and safety management;
- Environmental management;
- Strategic management;
- Information management; and
- Results based management.

Requirements for the reporting of mine action risk management aspects should be detailed at an appropriate level in:

- NMAS;
- Accreditation agreements;
- Donor agreements;
- Mine action organisations` SOPs; and
- Other relevant documentation.

Information to support the continual improvement of risk management in mine action should be communicated to relevant stakeholders as widely as possible, consistent with any limitations associated with contractual, commercial and other legal constraints.

8 Responsibilities

8.1 National Mine Action Authority/National Coordination Body

The NMAA, or an organisation acting on its behalf, shall:

a) establish, communicate and maintain policies, criteria and/or other guidance on the management of risk in mine action within the Mine Action Programme (MAP);

b) ensure that organisations working within the MAP establish risk management systems that are effective and appropriate within the prevailing circumstances and conditions;

c) specify the national standards and provide guidelines for the risk management of mine action organisations and activities;

d) review the management of risk within the MAP, at intervals appropriate to the prevailing situation and in any case at intervals of no more than twelve months;

e) ensure appropriate follow-up action is taken in light of the conclusions and recommendations of MAP risk management reviews; and

f) monitor the effectiveness of risk management carried out by mine action organisations, including sub-units, in accordance with IMAS 07.40.

8.2 Mine action organisations

Mine action organisations shall:

a) establish and maintain an effective and documented risk management system;

b) establish risk management policies, processes and procedures appropriate to the scope of the organisation's own activities and in compliance with any risk management policies and criteria established by the NMAA;

c) apply management practices, and risk management and operational procedures adequate to ensure the effective and efficient achievement of objectives;

d) maintain, ensure the accuracy and validity of, and make available, documentation (including SOPs and other written procedures), reports, records, and other data on their activities in accordance with IMAS 07.40;

In the absence of a NMAA or similar authority, the mine action organisation should assume additional responsibilities. These include:

a) agree with the donor (or client, or customer) a system for managing risk in mine action activities; and

b) assist the host nation, during the establishment of a NMAA, in framing national standards for risk management.

8.3 Donors, clients and other stakeholders

Those organisations contracting or funding mine action operations shall:

a) specify and agree their risk management criteria and other requirements to mine action organisations in clear and unambiguous terms; and

b) include details of risk management requirements, or in the absence of a NMAA, requirements established by the UN or other appropriate international body, in contracts, memoranda of understanding and other relevant documentation.

Annexes

A. Normative references
B. Risk management tools (informative)
C. Guidance Threat Analysis and Threat Assessment in Environments Affected by Improvised Explosive Devices (IEDs)

Annex A
(Normative)
References

The following normative documents contain provisions, which, through reference in this text, constitute provisions of this part of the standard. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of the standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid ISO or EN:

a) IMAS 04.10 Glossary of mine action terms, definitions and abbreviations;

b) IMAS 07.11 Land Release;

c) IMAS 07.12 Quality Management in Mine Action;

d) IMAS 07.13 Environmental Management in Mine Action;

e) IMAS 07.30 Accreditation of demining organisations and operations; and

f) IMAS 07.40 Monitoring of mine action organisations;

Annex B
(Informative)
Risk Management Tools

This Annex provides brief guidance on the use of a number of the most widely applicable and commonly used tools to support the application of the risk management process. Many other tools are available, and mine action risk managers are encouraged to explore options, make use of guidance found in other publications and on line, and apply those tools most suitable for the demands of their own projects and programmes.

ISO 31010:2009 Risk management – Risk assessment techniques (under ISO review for updating as of February 2019) provides a comprehensive guide to tools, their strengths and weaknesses and how to apply them.

The tools described in this Annex are applicable to different elements of the mine action risk management cycle as follows:

Ref	Tool	Context/scope	Risk Identification	Risk analysis	Risk evaluation	Risk treatment	Risk Review
B.1	Risk Register	X	X	X	X	X	X
B.2	PESTLE	X	X				
B.3	SWIFT		X	X	X		
B.4	SWOT	X	X			X	
B.5	Mine Action Architecture	X					
B.6	Consequence/likelihood matrix			X	X		
B.7	Bow Tie Analysis			X	X	X	

B.1 Risk register

The risk register provides the primary means of recording risks that have been identified, assessments of their significance, details of treatment measures and evidence that reviews have been conducted.

The risk register should be managed as a controlled document in accordance with Section 19 of IMAS 07.12.

Mine action managers may choose to adapt and adjust the layout of the risk register to reflect policies, requirements and circumstances related to their own mine action organisations, but it is recommended that any risk register include as a minimum:

- Details of the organisation, programme or project maintaining the risk register;
- Details of the person/job title responsible for ensuring effective implementation of the risk management system;
- Date on which the risk register was last reviewed;
- For each risk:
    - An identifying risk reference;
    - A risk category (e.g. Political, Economic, Safety, Environmental, etc.);
    - Description of the risk (e.g. road traffic accident; unplanned explosion at a munition site (UEMS) etc.);
    - An assessment of the likelihood of the risk event;
    - An assessment of the severity of the consequences of the risk event;
    - An assessment of the risk level;
    - Risk treatment (mitigation, reduction) measures associated with the risk;
    - Details of the person/job title responsible for ensuring that risk treatment measures are effectively implemented;
- The date when the register will next be reviewed (noting that some accidents, incidents or other significant events may trigger a review of the risk register at an earlier date).

Organisations may wish to include additional detail to reflect their own general management systems, as well as the application of other recognised risk management systems. Some organisations choose to include detail of the level of risk before and after implementation of risk treatment measures.

The contents of the risk register should be consistent with the scope of the risk management system as determined by the responsible mine action risk managers.

The risk register may be a simple table (in a word-processing or spreadsheet application), a dynamic database or held within a dedicated risk management App, many of which are available through online sources.

Diaries and other ‘bring-up’ systems should be used to ensure that risk reviews are conducted at appropriate intervals (in accordance with Section 7.6 of this standard).

B.2 'PESTLE' Analysis

Bringing a comprehensive and open approach to understanding external context is important to ensure that potentially significant, but unfamiliar risks and sources of risk, are not missed, ignored or forgotten. The PESTLE tool is used to help identify the external factors influencing a programme, organisation or project and the decisions it makes about its objectives and how to achieve them. The PESTLE headings stand for:

- **Political** - including, national, regional and local governmental, institutional, etc.;
- **Economic** - including commercial and financial;
- **Social** - including local communities, human resources and cultural aspects;
- **Technical** - including operational and technological aspects;
- **Legal** - including national, international, humanitarian, other laws, regulations, standards, etc.; and
- **Environmental** - including the natural and built environment.

What to use the tool for

The PESTLE approach can be used as an aid memoir/check list to help identify stakeholders/interested parties (as part of describing the context of a mine action organisation, project or programme), and as a framework for identifying risks.

Note: PESTLE can also be useful in support of many other management tools.

How to use the tool

PESTLE can be used during group meetings and to support desktop studies and other analysis of risks, systems, specific topics or issues and events.

Understanding context/scope:

- Determine the focus of the analysis (the entirety of a system, the development of a new regulation, an individual organisation's operations, an activity, a task, etc.);
- Decide whether it is necessary to split the analysis into different levels, such as:
    - Local, regional, national and international;
    - Strategic, operational, and technical; and
    - Risk education, land release, PSSM, etc.
- List stakeholders/interested parties/aspects relevant to the scope of the analysis under each PESTLE heading; and
- Consider associating additional detail with each entry – such as expectations, requirements, preferences, etc.

Identifying risk:

- Determine the focus of the analysis (an organisational element, an activity, a piece of equipment, etc.); and
- List risks under each of the PESTLE headings.

Benefits and limitations

PESTLE provides a widely applicable and easy-to-use way to encourage users to identify and consider issues, aspects and implications that may fall outside their normal day-to-day experience or focus.

PESTLE is focused on external environments/contexts and is not well adapted to analysis of factors inside organisations. If the scope is not well defined (and the analysis stays within the scope) PESTLE can become unwieldy with excessive information that is hard to analyse and understand.

B.3 Structured "What-if" Technique (SWIFT)

Asking 'what if' questions is a normal part of many risk management processes, sometimes as part of a more general brainstorming exercise. SWIFT brings a more structured approach than pure brainstorming to identifying and understanding risk. It allows participants in risk management processes to think through the implications of scenarios relevant to their organisations and activities.

What to use the tool for

SWIFT is applicable for almost all risk assessments. It is useful in risk identification, risk analysis and risk evaluation. The results of SWIFT analysis may also inform the development of risk treatment measures. SWIFT is often used to consider the implications of changes in situations.

How to use the tool

Identify the process, procedure or other aspect to be assessed. Before the SWIFT session or study starts a designated leader/facilitator prepares a list of prompt words or phrases (that may have been used before or are developed to reflect the specific focus of the session/study). SWIFT phrases typically include phrases such as:

- What if ….?
- What would happen if …?
- Could someone or something ….?
- Has anything or anyone ever ….?

The aim is to encourage the SWIFT session/study participants to explore potential scenarios, think through the events that could lead to such scenarios as well as the consequences of resulting risk events. During the SWIFT workshop, the context associated with the process, procedure or change should be discussed and agreed. The facilitator then asks participants to discuss:

- Known risks and hazards;
- Previous experience including incidents, accidents and other issues;
- Known and existing risk controls and their effectiveness;
- Associated SOPs, aid-memoirs, check lists and other documented guidance; and
- Legal, standards, regulatory and other associated requirements.

Each risk identified by participants is summarised and recorded (a risk register as recommended in this Annex can be used), with a description of its causes, consequences and current treatment.

Note: the Ishikawa/fishbone diagram and '5 whys' techniques may be helpful in exploring root cause aspects of identified risks.

The SWIFT participants consider whether the current controls are effective and, if necessary, agree an action plan (what will be done, by whom, by when?) to implement additional

controls. It may be useful to consider further 'What-if?' questions during this stage of the discussions.

Benefits and limitations

SWIFT can be a quick and efficient way of focusing on significant aspects of operations and activities. It is flexible and can be applied to many activities, processes, systems and procedures. It makes use of the experience of managers and staff members, as well as other relevant stakeholders and can produce clear action plans to improve the treatment of risks.

The benefits of SWIFT typically depend on the ability of the risk assessment leader/facilitator as well as on the knowledge of the participants. If the team fail to identify and ask important questions, they may miss potential problems. SWIFT usually yields qualitative results rather than quantitative ones.

B.4 SWOT

What to use the tool for

Strengths, Weaknesses, Opportunities and Threats (SWOT) analysis can help mine action managers understand important aspects of both the internal and external context within which they work. Advanced SWOT analysis can help develop appropriate risk treatments.

A SWOT analysis is best conducted by a group or team including representatives of as wide a selection of stakeholders as possible.

SWOT analysis is a key tool in the strategic planning process and may be applied in a range of other organisational, business and planning processes.

How to use the tool

B4.1 Basic SWOT for contextual analysis and risk identification

Strengths

Strengths are determined by internal factors. Questions to help identify underlying strengths can include:

- What activities do we do well?
- What aspects of what we do make us attractive to partners, customers, donors, beneficiaries?
- What assets and resources do we have that we could not do without?
- What factors have contributed most to our successes?
- What advantages do we offer over other organisations or programmes?
- What do our stakeholders see as our strengths?
- What specialised skills, techniques, equipment or methodologies do we use?

Weaknesses

Weaknesses are also determined by internal factors. Questions relating to weaknesses can include:

- What aspects, processes, elements need urgent improvement?
- Which factors have contributed most to our failures or problems?

- What limitations are preventing us from improving, expanding or making more of a difference?
- What factors have contributed to loss of bids, opportunities, customers, donors, etc.?

Opportunities

Opportunities reflect aspects of the external context. Questions relating to opportunities include:

- What could we be doing that we are not?
- Are there changes in the external context that create opportunities?
- Could we help address requirements that other organisations are struggling with?
- Are we fully reflecting the confidence of our external stakeholders and the needs they have?

Threats

Threats are a feature of the external context. Questions relating to threats could include:

- What external factors could stop our ability to work permanently or temporarily?
- What external factors could make it harder for us to work efficiently?
- Are there changes and trends in the security situation that may hinder or prevent our ability to work and succeed?
- Are there changes in the political, economic or legal landscape that may impact negatively on us?
- Are there social or cultural changes that may impact negatively on our ability to be effective and/or efficient in achieving our objectives?

Mine action managers should identify additional questions relevant to the scope of activities and risks for which they are responsible.

The results of the SWOT analysis are often captured in a simple matrix:

	Helpful (to achieving objectives)	**Harmful** (to achieving objectives)
Internal (attributes of the organisation)	*Strengths:*	*Weaknesses:*
External (attributes of the context)	*Opportunities:*	*Threats:*

B4.2 Advanced SWOT and risk treatment

In an advanced SWOT the relationships between the four components of the analysis are considered in order to:

- Take advantage of opportunities by using strengths; and
- Reduce weaknesses that may make threats a reality.

The results of such an analysis can be captured in a similar matrix:

	Strengths	Weaknesses
Opportunities	*How can strengths be used to take advantage of opportunities?*	*How can weaknesses that prevent taking advantage of opportunities be overcome?*
Threats	*How can strengths be used to reduce the likelihood and impact of threats?*	*How can weaknesses that may make threats a reality be overcome?*

The actions that arise from the advanced SWOT constitute risk treatments. They reduce the likelihood of negative events, they increase the likelihood of positive ones, and they reduce negative consequences and promote positive ones.

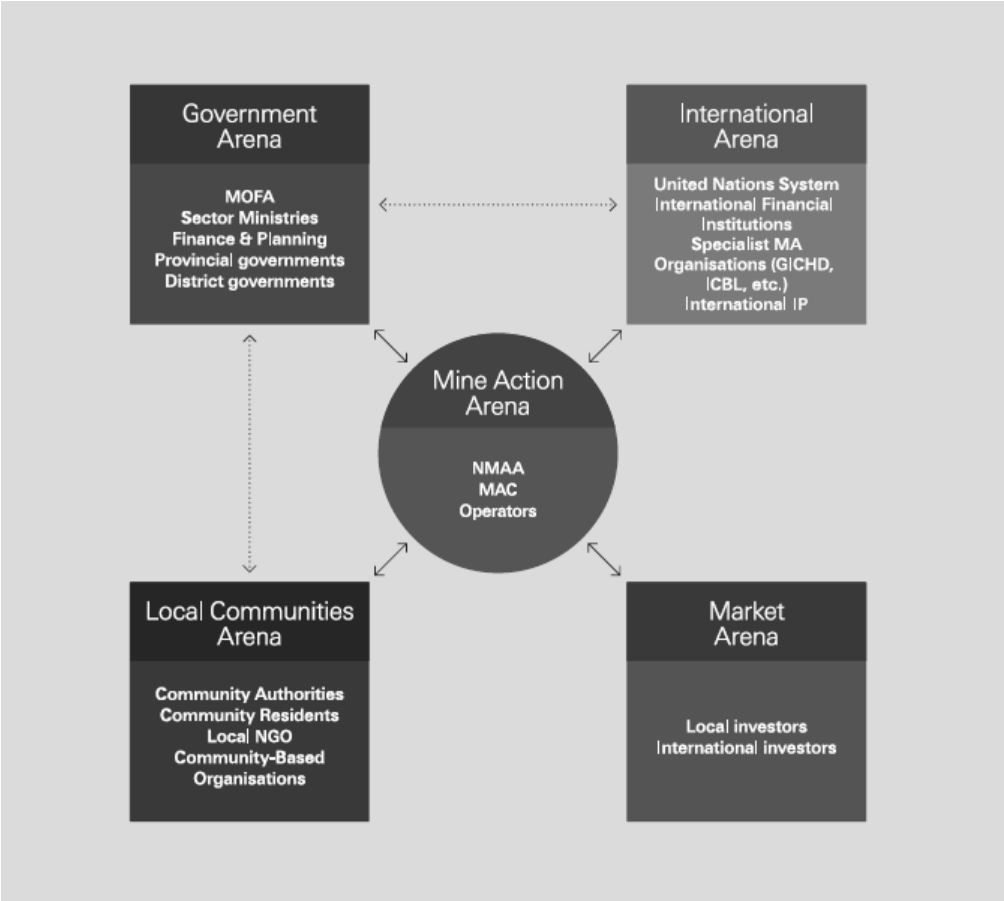
Benefits and limitations

SWOT analysis is easy to perform and anyone who has understanding of the organisation or element under consideration can perform the analysis. SWOT analysis helps stakeholders understand a programme or organisation better and can feed into the development of goals and objectives to support successful and improving operations.

SWOT analysis does not offer solutions on its own or prioritise actions, and there is a risk that it may generate a great deal of information, not all of it helpful. SWOT needs to be part of a wider risk management process. It may be difficult to determine how to categorise some factors.

B.5 Mine Action Architecture

The Mine Action Architecture diagram provides a succinct overview of the main categories of stakeholder associated with humanitarian mine action and the links between them.



What to use the tool for

The tool can be used to encourage risk managers, planners and meeting participants to maintain a broad perspective when identifying stakeholders as part of their assessment of external context and when considering the influence of those stakeholders on, and susceptibility to, mine action issues.

How to use the tool

Provide meeting participants with a copy of the architecture diagram and ask them to identify stakeholders, specific to their own organisations, programmes or projects from within the different 'arenas'. Results may be collected using a table with the titles of each arena as column headings.

The architecture diagram can be used in conjunction with a PESTLE analysis (section B.2 of this Annex) to identify and associate risks related to each arena, or individual stakeholders within arenas.

The mine action architecture diagram can be a useful support tool when engaging in a wide variety of other analyses at strategic, organisational, operational and technical levels when it is useful to encourage and maintain a broad perspective.

Benefits and limitations

The architecture diagram provides a simple aid memoir to help managers and meeting participants to identify stakeholders across all aspects of the humanitarian mine action sector, rather than only those that they are most familiar with. This can be particularly useful when working at the strategic level but may also be helpful when considering more operational or technical aspects that have the potential to influence, or be influenced by, issues arising from stakeholders outside the immediate view of managers.

The architecture diagram provides a high-level picture of the humanitarian mine action sector. To gain the full value of any stakeholder analysis process managers and meeting participants may need to drill down into much greater detail within the different arenas.

B.6 Consequence/likelihood matrices

Consequence/likelihood (C/L) matrices are widely used in the management of risk. This Annex does not require or suggest that the examples provided should be adopted in exactly the same format as presented here. Mine action risk managers should adapt the tool to best reflect their own circumstances and requirements.

What to use the tool for

C/L matrices do not usually produce absolute indications of risk level, but they do provide a structure within which different risks can be compared and ranked. C/L matrices provide a screening tool to evaluate those risks that require further treatment as opposed to those that do not (because they are already at a tolerable level). C/L matrices help bring a common approach to understanding, assessing and evaluating risk across an organisation. Risk criteria, relating to the level of risk that must be treated, may be treated, or that need not be treated should reflect the circumstances within which the organisation works and its attitudes towards risk.

C/L matrices can be applied to any category of risk (political, environmental, safety, etc.), but will need different descriptions of the levels associated with the matrix scales in each case.

How to use the tool

Structure of the C/L matrix

The C/L matrix is formed with two scales – one for probability/likelihood of an event; the other for severity/consequence. The scales may have any number of levels, but 3, 4, 5 or 6 are most commonly used. Scales may be based on narrative or quantitative descriptions.

Within the matrix, levels of risk are determined for each score combination. The matrix may be set up to give more weight to likelihood or consequence, or it may be symmetrical. Levels of risk may be linked to decision rules relating to whether management must take action to treat the risk and other factors, such as how quickly action must be implemented.

Using the C/L matrix

The table below provides an example of C/L scales relating to human safety aspects. Similar matrices can and should be developed for other categories of risk using different scales for severity and, if necessary, for likelihood.

	Severity	**Description**		**Likelihood**	**Description**
1	Delays	Damage to equipment, re-routing of site access	**1**	Almost impossible	It is almost impossible to envisage this happening
2	Minor injury	Scratches and bruises, minor burns, sprains and strains, fractures of digits, dizziness, cuts, abrasions	**2**	Very unlikely	The event has never happened or is very rare. There is no expectation that this will happen
3	Single major injury	Fractures of hand, wrist, ankle, major burns, unconsciousness, amputation of digits, temporary loss of sight/hearing	**3**	Unlikely	It is known that this event has happened. We recognise this could happen, but we do not expect it to
4	Multiple major injury	Multiple major injuries to one person, multiple persons with one or more major injury	**4**	Possible	This event occurs infrequently. This might happen and is feasible
5	Fatality	One or small number of deaths	**5**	Probable	It is fairly likely that this will happen
6	Multiple fatalities	Large number of deaths	**6**	Very likely	This event occurs frequently. We expect this event to happen

In some cases, it may be possible to associate numerical percentage risk scales with the likelihood of risk events, although it is often not possible to do so in mine action situations. Mine action risk managers should liaise with information managers to identify aspects that may be suitable for quantitative analysis.

The C/L matrix below provides an example of how the two scales can be combined and associated with risk levels (Low, Low-Medium, Medium, Medium-High and High). C/L matrices are often coloured-coded to improve clarity.

		Likelihood						
		1	2	3	4	5	6	
Severity	1	L-M	M	M-H	H	H	H	1
	2	L-M	M	M	M-H	H	H	2
	3	L	L-M	M	M	M-H	H	3
	4	L	L	L-M	M	M	M-H	4
	5	L	L	L	L-M	M	M	5
	6	L	L	L	L	L-M	L-M	6
		1	2	3	4	5	6	

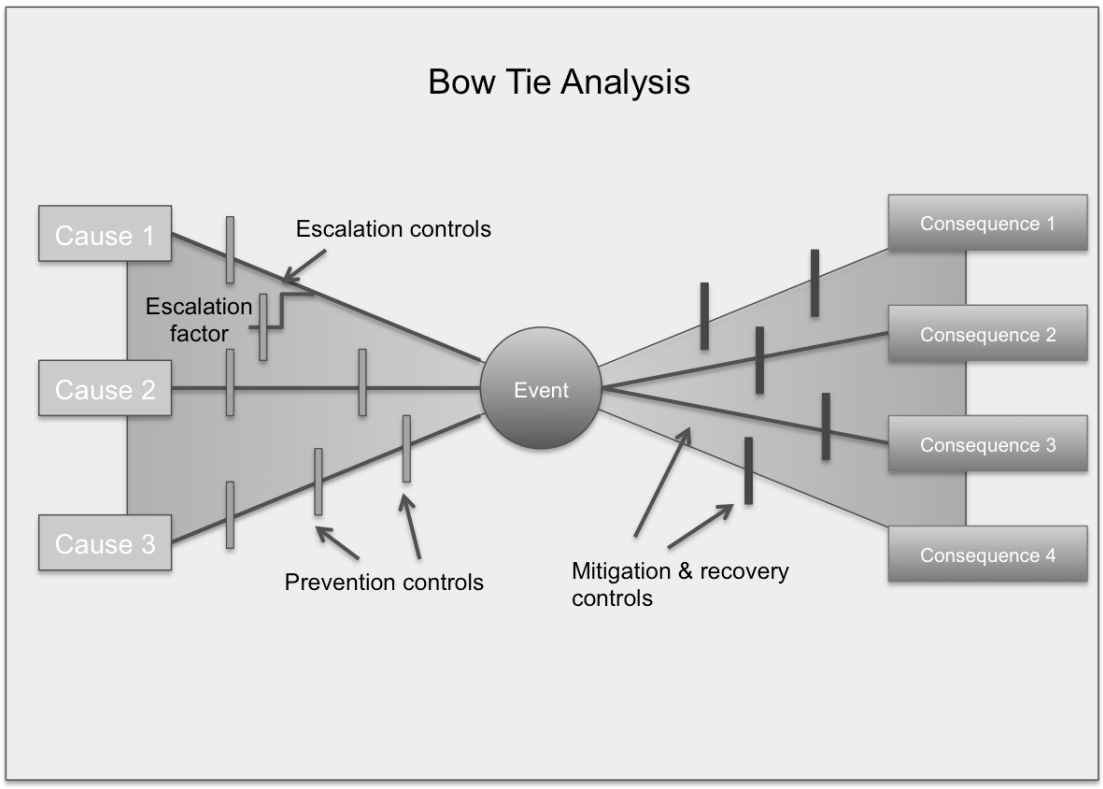
Note: There is no standard as to how significance levels should be distributed across the matrix. Mine action risk managers should agree, with relevant stakeholders, an approach that is appropriate to their own circumstances and conditions.

Benefits and limitations

C/L matrices are relatively easy to use and provide a rapid ranking of risks into different significance levels.

It can be difficult to define C/L matrix scales unambiguously and use can be subjective. There may be differences in the results provided by different individuals or groups when rating the same or similar risks. C/L matrices vary between organisations.

B.7 Bow Tie Analysis



What to use the tool for

Bow Tie analysis is useful for analysing events that may have more than one possible cause and that can have a range of consequences.

How to use the tool

The bow tie diagram can be drawn direct from a brainstorming session:

- A risk is identified for analysis and is placed at the central knot of the bow tie;
- Risk causes (hazards in a safety context) are listed and the mechanisms by which they give rise to the risk are discussed and described;
- Lines are drawn between each cause and the risk;
- Factors which could escalate the situation can also be included on the left-hand side of the diagram;
- Barriers which could prevent a cause leading to the central event are identified and represented as vertical lines cutting across the relevant cause line;
- Barriers to escalation can also be included as vertical lines in the left side of the diagram;
- On the right-hand side of the diagram consequences are identified and listed, with consequence lines leading out from the central event; and
- Barriers that prevent or mitigate consequences are shown as vertical lines cutting across the relevant consequence lines.

Benefits and limitations

Bow tie analysis provides a simple, easy to understand diagrammatic representation of a risk, its causes, consequences and possible controls.

Users should be careful to ensure that the analysis does not oversimplify more complex situations.

Annex C
(Informative)

Threat Analysis and Threat Assessment in Environments Affected by Improvised Explosive Devices (IEDs)

Scope

The purpose of this annex is to outline the processes and outputs related to the implementation of Threat Analysis and Threat Assessment in environments affected by Improvised Explosive Devices (IEDs). Threat Analysis will address the broader national and regional contexts and will consider threats that exert influence at the macro level. The threat analysis will also address the security situation involving armed actors and their IED capabilities, which will assist in decision making for mine action actors assessing the need and whether conditions are suitable for intervention. Threat Assessment is informed by the broader Threat Analysis, addressing a specific operational task. Both Threat Analysis and Threat Assessment will be informed and will feed into other IMAS processes, such as Land Release (IMAS 07.11) and Non-Technical Survey (IMAS 08.10) when there is a suspicion that IEDs are present.

Purpose of Threat Analysis and Threat Assessment

The purpose of Threat Analysis and Threat Assessment is to provide MA stakeholders with an up-to-date and accurate assessment of the threats that are present in environments affected by IEDs. They will support reliable and effective decision making in relation to strategic, operational, technical and safety planning. These assessments also inform the management of longer term risk to organisational operations and reputation in country.

Both Threat Analysis and Threat Assessment use all appropriate non-intrusive means, including visits to field locations, to identify, collect, analyse and report information/evidence in order to produce a threat summary which will:

- assist in the production of a general assessments[3]
- make recommendations about the definition of SHAs/CHAs;
- support priority setting processes;
- support the cancellation and/or subsequent reduction/clearance of areas;
- contribute to the efficient and effective planning of subsequent technical interventions;
- Inform organisational risk thresholds i.e. risk levels at the level of organisation below that require escalation to the NMAA

Relationship between Threat Analysis, Threat Assessment and Risk Management

Risk is the effect of uncertainty on objectives and Threat Analysis and Threat Assessment use analytical methods to manage the uncertainty around a threat and choose appropriate risk responses. As such, Threat Analysis and Threat Assessment are both part of the MA Risk Management System. While threat and risk are closely and often interrelated, risk is the product of the threats that exist and the probability of occurrence of harm. Threats can be passive, but in regards to the employment of IEDs include the malicious human intent that will influence the nature and severity of the threat. This is a distinction made in multiple sectors that are involved in different areas of security such as cyber security, studies into nuclear non-proliferation and physical security.

The key elements of the risk management process (IMAS 07.14 section 7), which are drawn from ISO 31000, are also present in Threat Analysis and Threat Assessment (ISO 27001).

[3] This level could be included as part of assessment for mine action intervention at the earliest opportunity, as per IMAS 02.10. This process can also be used at the national, regional and local levels.

Each process focusses on these points at a level appropriate for their strategic or operational aims:

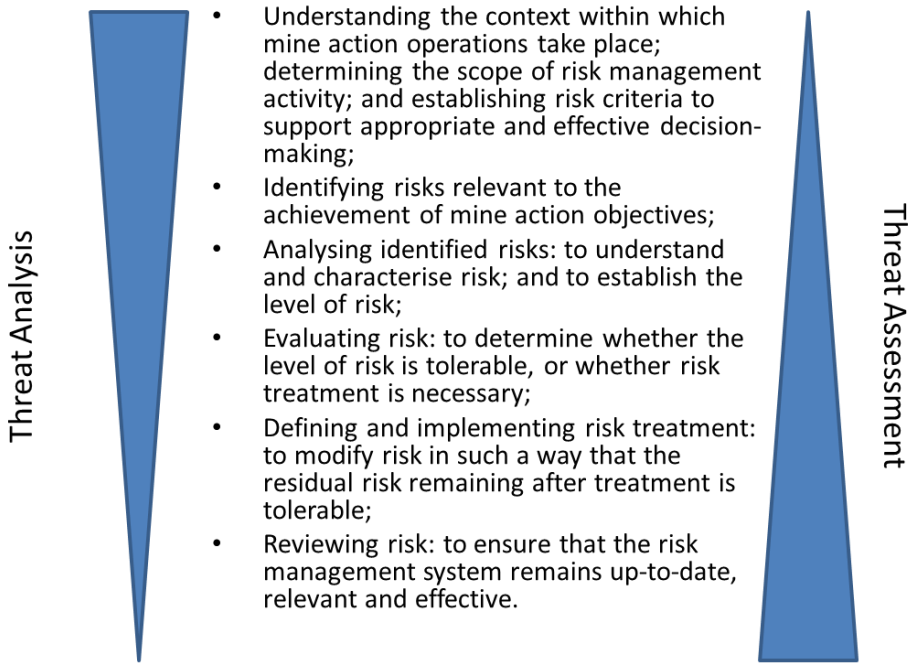


Figure 1: Diagram showing a representative distribution of effort of Threat Analysis and Threat Assessment processes against the key elements of Risk Management. This is assuming that the Threat Analysis is performed such that the Threat Assessment does not have to revisit the earlier points established in the threat analysis summary in detail, instead they can extract the detail directly.

Threat Analysis for National Planning

Threat Analysis at the National level should be used before the establishment of a mine action programme in a specific country or region, to understand the operating context and identify space for humanitarian interventions and prioritisation of tasks. The breadth, depth and scope of such analysis at the National Level can be represented through taking a PESTLE approach:

- What is the political situation of the country and how can it affect mine action?
- What are the prevalent economic factors?
- Identify relevant cultural and social factors and their determinants?
- What technological issues are relevant?
- Are there any current legislations that regulate mine action or will there need to be any change in the legislations for the sector?
- What are the environmental concerns?

The political, economic, social, technical, legal and environmental factors should all be considered to define the necessary approach for safe and effective operations. Considering this variety of drivers allows identification and appraisal of areas of exposure that can then be mitigated though appropriate permissions, planning and deployment of resources.

Figure 2: An example of elements to consider in a National Threat Analysis, represented through PESTLE.

The National analysis of IED contamination in a country will make use of the multiple information sources that feed the PESTLE approach above, to varying degrees. The summary and other findings from this analysis will feed back into the PESTLE, primarily on Technical and other aspects regarding security in the Political considerations. This will support the decision making processes in IMAS 02.10, “Guide for the establishment of a demining programme” (section 5 - Mine action programme establishment considerations).

In more specific detail relating to IEDs the following elements can be considered in the elaboration of the Threat Analysis.

External Reports

These reports, while they may not have the detail of specific devices, may hold valuable information that could provide indirect evidence for device types and emplacement. The following are examples that may be found within other organisations which may hold relevant information for both the analysis and assessment processes:

- Explosive incident reports
- General security reports
- Casualty data
- Remotely delivered weapons data (bombing, artillery, guided)
- Conflict phases
- IDP/refugee movements

The following information should be extracted from available reporting where possible:

- Location information including GPS coordinates of incidents and seats of the explosion.
- Photos or descriptions of the site of the incident and damage inflicted.

- Casualty information including ethnicity, allegiance, age, gender, religion, injuries sustained.
- Activities of people involved leading up to the incident.
- Last known date of fighting/occupation by armed actors.
- IDP information including ethnicity, allegiance, age, gender, religion, why they were forced to leave an area and how were they treated by different armed groups.

Internal Reports

These types of reports are expected to be held and used by mine action organisations. For them to be of use in threat assessment they should be available in real time to all MA operators.

- Community Liaison
- Non-Technical Survey (NTS)
- Spot task
- Completion
- Device technical reports

These combined reports will have relevant information that will provide both indirect and direct evidence on device types and their emplacement (including coordinates and photos). Information will be of greater relevance due to the nature of the reports but will include:

Detailed information on device type and switching:

- Detail of 5 main IED components:
    - Switch or switches
    - Main charge
    - Initiator
    - Power source
    - Container
- Where devices have been deployed and how have they been camouflaged.
- Their potential to function over time.
- Identifying features such as materials used
- Potential targeting of those attempting to find and render safe devices.
- The capability of current procedures and equipment to mitigate the threat.

Threat context

The threat analysis involves breaking down the conflict in general to provide a detailed threat picture of the situation. While similar to the threat assessment, the product is a wider general summary of the conflict situation in regards to IEDs rather than a judgement based on detailed evidence. When applied to an ongoing conflict, this must be updated regularly as conflict lines and tactics and procedures change. Any assessment should be reviewed when there has been a change to the contributing information that was used to make it. The following are the main areas for consideration when conducting threat analysis.

Geographical area to be covered

When conflicts take place in areas that have multiple environment types, the tactics and procedures of employing ERW including IED's may vary considerably. These differences may affect the device types and their physical position when used against different targets. To conduct threat analysis in regions that are in or post conflict, the analysis should include the geographical information at the following levels:

- national
- regional
- local
- operational

State of the conflict

The state of the conflict is important when mapping and understanding the threat. Territory may change hands multiple times and the alliances and focus of armed groups may change over time. It not only has a direct bearing on the permissiveness of the operating environment but also provides a timeline for when the last IEDs are likely to have been positioned in a defined geographical area. The state of the conflict itself may not assist in the determination of the most likely device type but will help identify areas where devices may still be functional.

Threat Mapping

Threat mapping is the product of transferring the information from the threat analysis summary over mapping or satellite imagery to provide a visual representation of the data to aid in the planning of operations. It can then be used by the relevant authority to focus on areas where operators could realistically carry out clearance, and if general security is sufficient, the integrity of that clearance can be maintained. Operators can also use this as the baseline for desktop studies for the safe and efficient deployment of teams for survey and clearance tasks. At the operational level, this will be used as the foundation from which a detailed threat assessment can be developed.

Armed actor mapping

In conflicts, especially those that involve one or more Non-State Armed Groups (NSAG), their potential targets may differ from area to area and in different phases of the conflict. It is therefore critical to identify all state and non-state armed actors, Identify the intention/motivation of each of the armed groups and any possible links/ alliances that they may have to internal or external groups (passage of information/technology). Groups may be broken down by ethnicity, political beliefs, tribal memberships, religious beliefs, or language.

Intent
Intent should be considered at multiple levels, starting with the global or national levels of the group. At the operational level, the effect on the specific target and what this will achieve are the items of information of most importance. The motivation of each actor in the conflict may not be straightforward to understand, especially amongst a confederation of different actors. In the case of more organized groups, there may be a political agenda or criminal intent.

Capability
Through data collection from various sources (victim investigation, post-blast analysis, and weapons information reports) information should be gathered on each armed group and establish their modus operandi and gather detailed information on each group's Tactics Training and Procedures (TTP). The information is often collected from reports of previous attacks or attempted attacks attributed to the armed groups or individuals within those armed groups, finds of bomb-making equipment and factories, personal accounts and knowledge of resources available. The capability of each actor will differ and could have a significant impact on if, how and by who the clearance is conducted.

Threat analysis summary

Threat analysis is a current explanation of the analytical findings based on the information collected. It should include all threats identified and address the following statements;

- History of current and previous conflicts
- Has the conflict moved far enough away for a suitable amount of time for an area to be considered permissive?
- Define the armed group being assessed
- Identify the boundaries of the group’s operations
- In placing the devices which group(s) are they targeting directly and affecting indirectly?

- Why are they targeting the individuals or groups identified?
- Identify the nature of the items they are using to conduct their attacks?
- Does the group identified use secondary devices or follow up with complex attacks?

A suggested template for the threat summary is shown below:

(Organisation name) operating in the ***(insert area of Place Name)*** is seeking to ***(insert Mission Statement)***. Currently operating in this area are ***(insert details of active groups)***. Their current targeting methods are comprised of ***(insert what targets they are attacking, i.e., patrol/vehicle/foot mounted/exactly where/slow down points/halts, etc.)***. The primary threat is likely to be ***(insert types of devices know to be used, i.e., CW/TD/VO/RC initiated blast fragmentation/incendiary/etc.)***. Devices range from ***(insert size of main charges and types of explosives)*** and are contained in ***(insert Packaging/composition)*** concealed in ***(insert likely locations)*** in relation to ***(insert target/in relation to geographical feature/camouflage)***. The methods of initiation known to be used are ***(insert details/direction/firing points/concealment/length of CW/depth of CW/description of components)***. ***(Insert direction of firing point from target to method and direction of extraction if relevant).***

Secondary threat: ***(Insert details of secondary threat such as targeting of Security forces EOD teams or emergency response teams in ICP. Attacks on target/cordon etc.)***.

Threat assessment process

Threat assessment is the process of gathering, analysing and interpreting information to produce a threat summary which will detail the most likely type of IEDs that would have been employed in a specific geographic area. It involves the triangulation of information available and finding the potential relationships or links between seemingly unrelated data, when considered in isolation. It is a process of elimination in which all possible device types must be considered and if they cannot be reasonably eliminated as a threat must be included in the threat summary. This differs from the standard risk assessment conducted during the Land Release process. The difference is in the level of analysis required of intent, opportunity capability. In the standard Land Release process, in a more stable security setting, there is a focus on risk (or 'threat') posed by the device, but the wider threat assessment is also understanding the intent of the combatants and why they would have laid a minefield or IED in a certain part of the hazard area, or where EO is most likely to be found.

Spot Tasks

Threat assessment can be applied to an area that requires clearance or to a spot task where the device type/suspicious object are yet to be confirmed and it may be positioned in a way that does not fit the trends of previous devices. In this case there is a greater focus on analysing the known intent and opportunity fields below and applying the assessment to not only the known but also the potential capabilities of an armed group as the device may be new and unreported. This summary shall then be used to identify the equipment and procedures required to carry out safe and efficient clearance and may vary, especially in different physical environments.

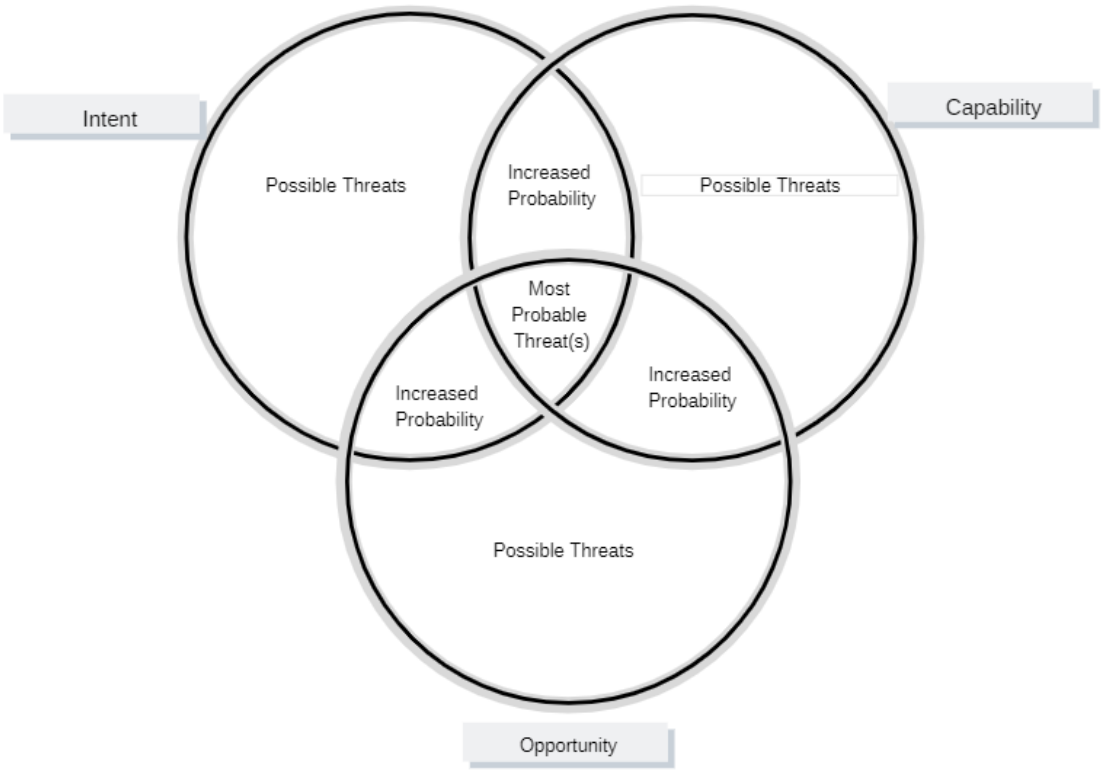


Figure 3: Intent, Capability and Opportunity

The diagram above shows three main fields for consideration when trying to determine the most likely threat(s). As information is cross-referenced from different fields the likelihood of the presence of specific device types increases.

Intent

Intent should be considered from the perspective of the armed actor to identify as far as possible the following information:

- Assessment of armed actors in conflict: Intent – Global, national, regional, local, operational
- Level of acceptance of non-intentional casualties
- Options for escape – escape routes, standoff from attacks allowing the use of command devices
- Who/What was the target:
    - Security forces, civilian, NGO
    - A building, infrastructure, event
- What effect did they want to achieve
    - Strategic: Fear, widespread support, destabilise the government, disrupt security situation, publicity,
    - Physical: Kill, injure, damage, destroy, hoax (gaining publicity especially)

Capability

An armed actor may have access to a wide variety and quantity of devices but will consider the effect they want to have and then choose the best device type to achieve this effect. The armed actor may make this decision after studying the behaviour of the target or assessing any potential patterns or weaknesses. The choice of switching for a device will therefore also be influenced by the opportunity presented by potential targets.

- How would they prepare the attack?
    - Resources, personnel, training, freedom of movement, local support, emplacement/camouflage of devices,
- How would they achieve the effect?
    - Switch: Time, Victim, Command
    - Main charge: Blast, fragmentation, EFP, incendiary, chemical, secondary device (first responders/clearance activities)

Opportunity

The opportunity is vital in identifying possible areas where a device may have been employed, especially a timed device. For a timed device to be used against a specific target, there must be a "window" of opportunity, and the target is presented at a known time for a reasonable amount of time for the device to be successful. IED's in general have multiple possibilities in switching, and the analysis of the patterns or weaknesses of the target and their environment will have significant impact in informing the possible type of switch used:

- Where would the attack(s) happen?
    - Does the ground lend itself to a specific type of device e.g. soft ground for pressure pads, high ground for command devices.
- Vulnerable areas – roads, area, buildings used by target, dominated by high ground
- Vulnerable points - access points, slow down points, culverts, bridges, stop for a break/fuel/lunch/work
- Possible escape routes for an armed actor after firing a command device
- When would they happen?
    - Pattern of life/pattern of work
    - Not just "time" specific – on way to work, back from work, at work. When the door is opened, when the item is picked up, "during the event"
    - When did the target present itself?
    - How long was the target presented for?

Threat Summary

Once all available information has been analysed, and the most likely threat(s) are assessed, a threat summary is produced. The assessment identifies the most likely type(s) of the device and where they are likely to be positioned. This summary will also help define the clearance parameters and therefore the procedures to be used in the clearance. The summary should be reviewed whenever there is a change to the original information (from whatever source) used to make the assessment. This may include information from witnesses, reports or from physical information discovered during the task.
Threat summary Structure

- Intent
- Capability
- Opportunity

"The armed actor intended to kill/injure civilians through the use of VOIED (most likely PPIED) emplaced in soft ground near doorways, in order to disrupt the reoccupation of the area."

The armed actor intended to damage or destroy the limited amount of heavily armoured vehicles available to security forces through the use of CIED (most likely CWIED with EFP) at junctions as they carried out patrols along roads in order to destabilise the security situation.

The Risk Management Cycle and Threat Analysis and Assessment

The Risk Management Cycle maps directly onto Threat Analysis and Threat Assessment:

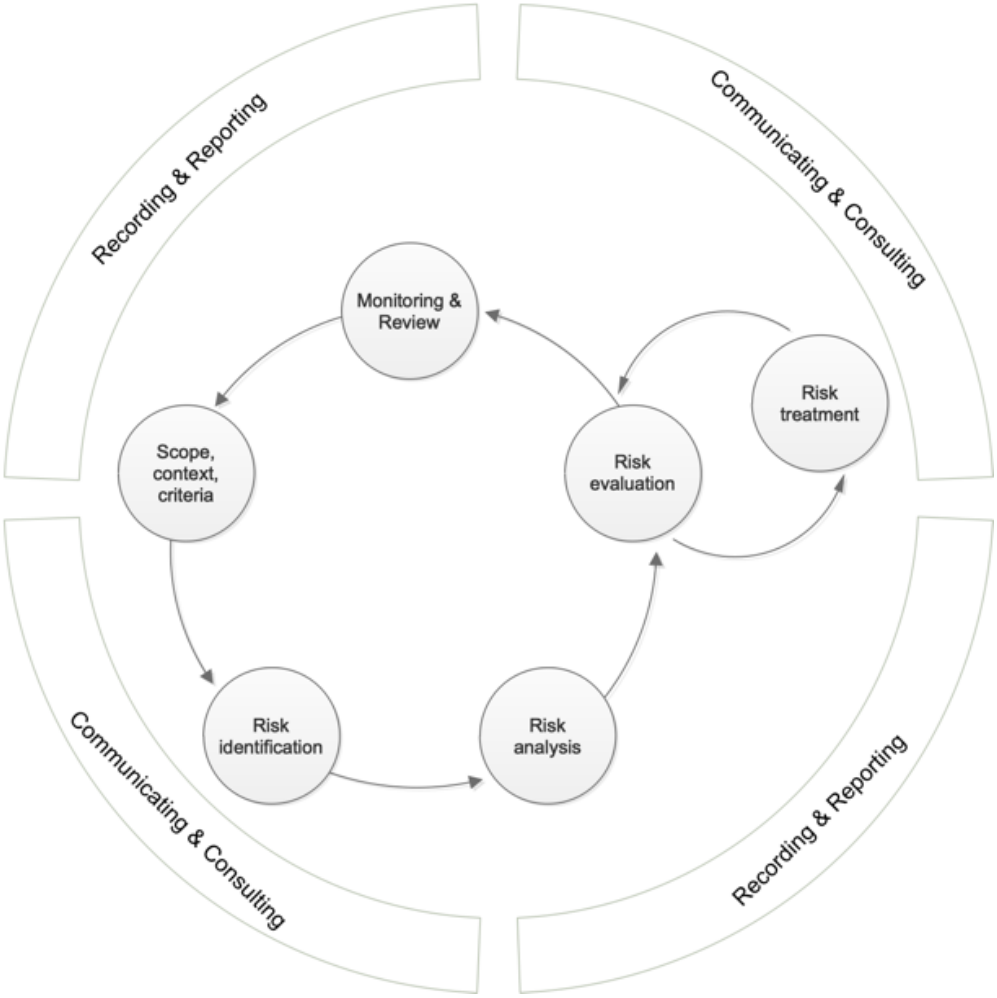


Figure 4: Risk Management Cycle

The key point often overlooked in this diagram is “Monitoring and Review”. If a risk is identified, analysed, evaluated and then not reviewed again when appropriate it means the risk treatment is potentially no longer suitable. In a highly complex and fast developing environment, this cannot be left to a periodic review of all risks. As described in the principle “dynamic and responsive” a risk management system should be able to improve, adjust and respond at a rate appropriate to changes in the internal and external context. To achieve this it has to be clear what circumstances should trigger a review and what actions are to be taken when triggered to ensure the review is completed in an appropriate timeline. In general there should be a review, whenever there is a change to the contributing information that was used to conduct the assessment.

Alignment with ISO standards

The key elements of a Risk Management System are drawn from ISO 31000 Risk Management, but due to the nature of the risks around EO including IEDs and the presence of malicious actors and intent to harm, the Risk Identification and Analysis are more closely aligned to ISO 27001 Information Security Management Systems.

Operational Threat Assessment

The priority for demining organisations as they form a mine action programme should be to conduct a threat analysis at a National level. This analysis will pull important and relevant information regarding the IED threat from multiple sources and be used to create more detailed threat analysis at the regional and local levels. These should all be made available to operators so that the information can be used in Threat Assessment at the operational level.

Threat assessment should be used to support planning and conduct of all mine action field activities, including all types of survey, clearance and community engagement. New information on EO contamination (including IED) could unexpectedly be gained at any time while conducting these activities e.g. from a participant during risk education. This can then be used to feed into the threat analysis and assessment processes.

Operational Threat Assessment

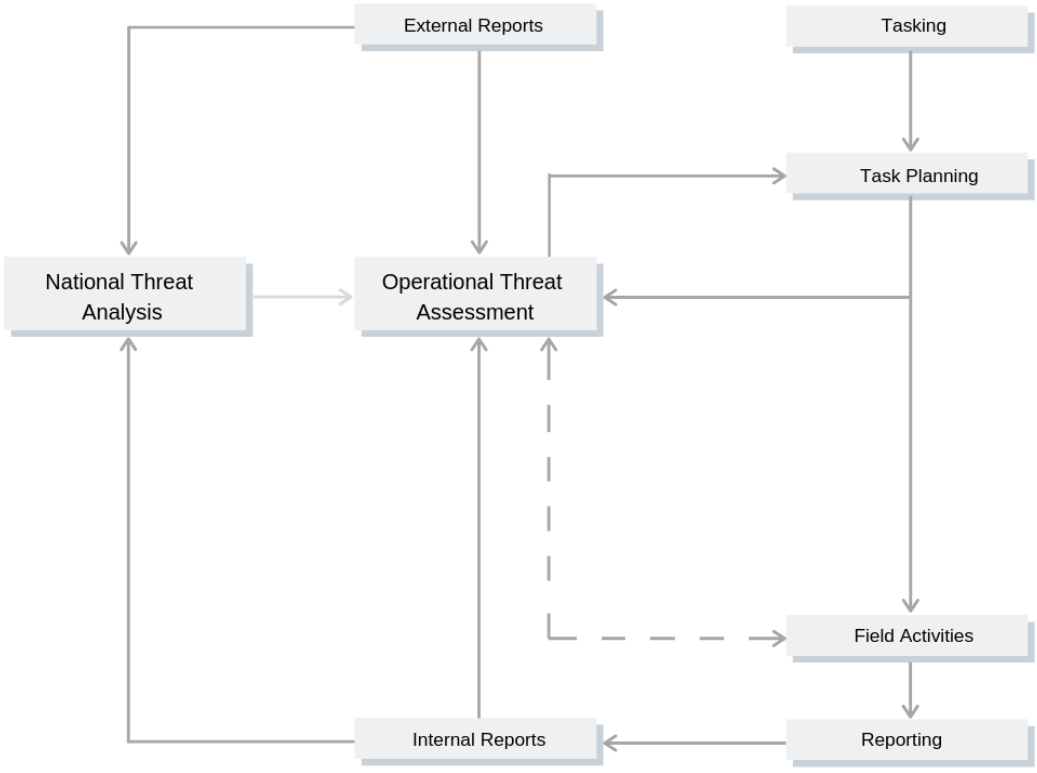


Figure 5: Operational Threat Assessment Process

Desktop study (as part of task planning)

The desktop study forms an essential part of task planning. All available documentation and threat/security mapping is explored to find interrelated information.

- GIS
- Time and distance assessment, to evaluate functional or non-functional
- Ground – Does the area lend itself to a type of IED, vegetation, buildings, low ground, high ground, hard ground, soft ground, known safe routes, CP locations
- Ethnic/cultural/allegiance makeup of the area.
- The current security situation, the location of checkpoints, the point of contact for the task or community, safe routes, armed actor activity (all factions), identification of humanitarian space.
- Previous task sites in the area and any contamination found.

- Previous IED incidents in the area, activity leading to the incident, security forces, LN civilians, NGO's, armed actor(s) acceptance of unintended casualties.
- Previous IED/UXO threat, technical data including device type, switch(es) and method of emplacement/concealment, number of devices, to inform on resources available to actors.
- Identify who/what were armed actors targeting
- Secondary hazards (especially for infrastructure) - Power, chemicals, enclosed spaces.
- Conflict timeline and areas of known fighting or occupation by armed groups

Field activities in IED contaminated environments (Non-Technical Survey)

When conducting NTS staff must exercise extreme caution, especially at the outset of a humanitarian mine action response as innocuous items may be part of or contain an IED. The following information should be gathered or confirmed from the NTS including the desktop study:

- Confirmation of safe routes, Limit of the safe area,
- Direct and indirect evidence of the presence or suspicion of IED's.
- Assessment of site, high ground, hard ground, soft ground, vegetation, obstacles and does it lend itself to a specific type of device.
- Additional hazards such as; enclosed spaces, working at height, chemicals.
- Confirm the use of buildings and areas prior, during and post-conflict.
- Damage to buildings such as signs of fighting, indirect attack and possible IED contamination.
- 360° of outside of task site if applicable and safe to gather imagery and define HA.
- Interview with site owner or qualified professional (infrastructure) if applicable.
- Interview locals including security forces if possible regarding security situation and EO contamination including IEDs.
- Use of UAV for site survey imagery if the site is inaccessible (may be intrusive if approved).