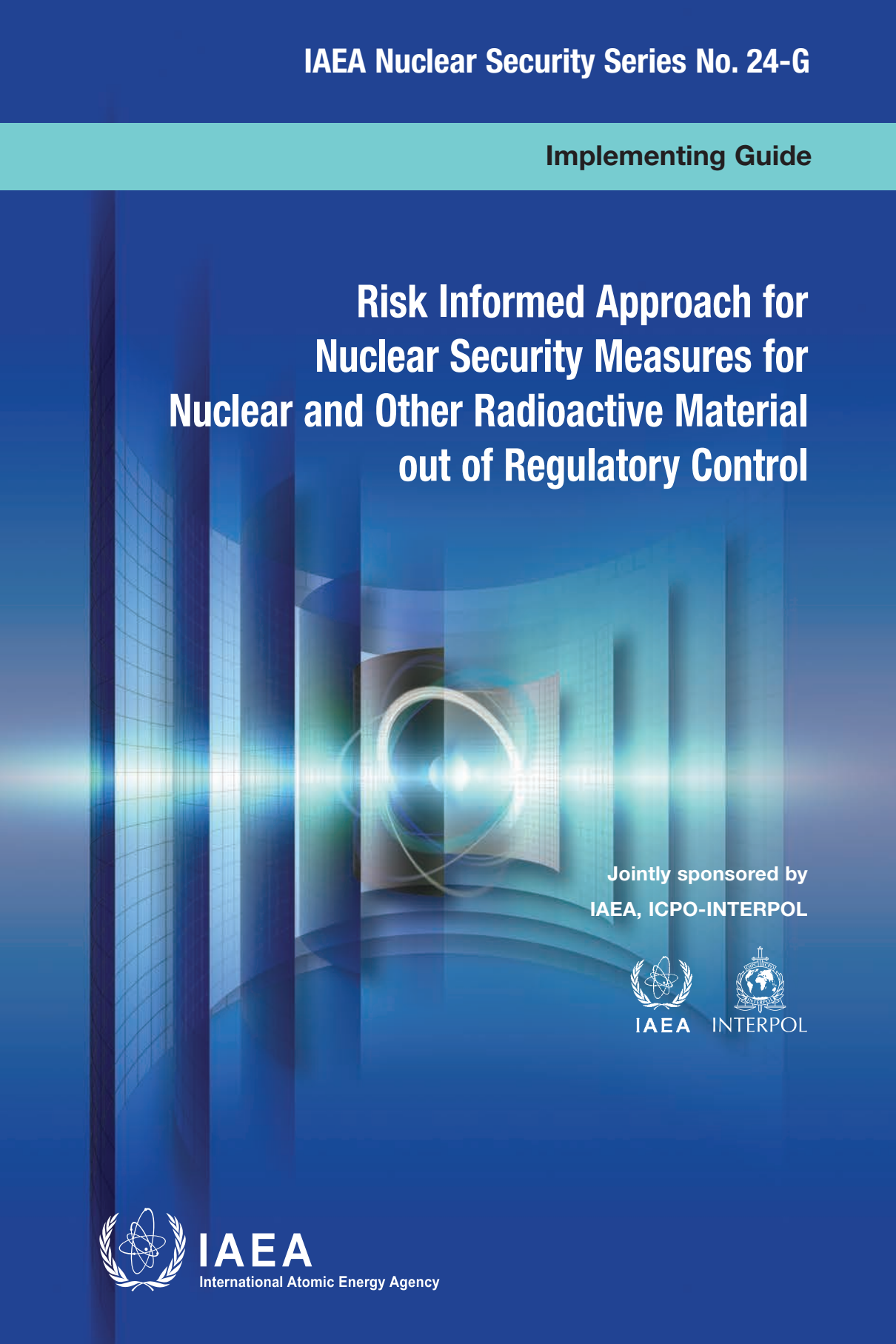
IAEA Nuclear Security Series No. 24-G

Implementing Guide

Risk Informed Approach for Nuclear Security Measures for Nuclear and Other Radioactive Material out of Regulatory Control



Jointly sponsored by
IAEA, ICPO-INTERPOL

IAEA INTERPOL

IAEA
International Atomic Energy Agency

IAEA NUCLEAR SECURITY SERIES

Nuclear security issues relating to the prevention and detection of, and response to, criminal or intentional unauthorized acts involving, or directed at, nuclear material, other radioactive material, associated facilities or associated activities are addressed in the **IAEA Nuclear Security Series**. These publications are consistent with, and complement, international nuclear security instruments, such as the Convention on the Physical Protection of Nuclear Material and its Amendment, the International Convention for the Suppression of Acts of Nuclear Terrorism, United Nations Security Council resolutions 1373 and 1540, and the Code of Conduct on the Safety and Security of Radioactive Sources.

CATEGORIES IN THE IAEA NUCLEAR SECURITY SERIES

Publications in the IAEA Nuclear Security Series are issued in the following categories:

- **Nuclear Security Fundamentals** specify the objective of a State's nuclear security regime and the essential elements of such a regime. They provide the basis for the Nuclear Security Recommendations.
- **Nuclear Security Recommendations** set out measures that States should take to achieve and maintain an effective national nuclear security regime consistent with the Nuclear Security Fundamentals.
- **Implementing Guides** provide guidance on the means by which States could implement the measures set out in the Nuclear Security Recommendations. As such, they focus on how to meet the recommendations relating to broad areas of nuclear security.
- **Technical Guidance** provides guidance on specific technical subjects to supplement the guidance set out in the Implementing Guides. They focus on details of how to implement the necessary measures.

DRAFTING AND REVIEW

The preparation and review of Nuclear Security Series publications involves the IAEA Secretariat, experts from Member States (who assist the Secretariat in drafting the publications) and the Nuclear Security Guidance Committee (NSGC), which reviews and approves draft publications. Where appropriate, open-ended technical meetings are also held during drafting to provide an opportunity for specialists from Member States and relevant international organizations to review and discuss the draft text. In addition, to ensure a high level of international review and consensus, the Secretariat submits the draft texts to all Member States for a period of 120 days for formal review.

For each publication, the Secretariat prepares the following, which the NSGC approves at successive stages in the preparation and review process:

- An outline and work plan describing the intended new or revised publication, its intended purpose, scope and content;
- A draft publication for submission to Member States for comment during the 120 day consultation period;
- A final draft publication taking account of Member States' comments.

The process for drafting and reviewing publications in the IAEA Nuclear Security Series takes account of confidentiality considerations and recognizes that nuclear security is inseparably linked with general and specific national security concerns.

An underlying consideration is that related IAEA safety standards and safeguards activities should be taken into account in the technical content of the publications. In particular, Nuclear Security Series publications addressing areas in which there are interfaces with safety — known as interface documents — are reviewed at each of the stages set out above by relevant Safety Standards Committees as well as by the NSGC.

RISK INFORMED APPROACH FOR NUCLEAR SECURITY MEASURES FOR NUCLEAR AND OTHER RADIOACTIVE MATERIAL OUT OF REGULATORY CONTROL

The Agency's Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world''.

IAEA NUCLEAR SECURITY SERIES No. 24-G

RISK INFORMED APPROACH FOR NUCLEAR SECURITY MEASURES FOR NUCLEAR AND OTHER RADIOACTIVE MATERIAL OUT OF REGULATORY CONTROL

IMPLEMENTING GUIDE

JOINTLY SPONSORED BY THE
INTERNATIONAL ATOMIC ENERGY AGENCY AND THE
INTERNATIONAL CRIMINAL POLICE ORGANIZATION–INTERPOL

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2015

COPYRIGHT NOTICE

Marketing and Sales Unit, Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
fax: +43 1 2600 29302
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
http://www.iaea.org/books

Printed by the IAEA in Austria
June 2015
STI/PUB/1678

IAEA Library Cataloguing in Publication Data

Risk informed approach for nuclear security measures for nuclear and other radioactive material out of regulatory control : implementing guide. — Vienna : International Atomic Energy Agency, 2015.
p. ; 24 cm. — (IAEA nuclear security series, ISSN 1816–9317 ; no. 24-G)
STI/PUB/1678
ISBN 978–92–0–100315–7
Includes bibliographical references.

1. Radioactive substances — Safety measures — International cooperation. 2. Radioactive substances — Security measures. 3. Nuclear facilities — Security measures. I. International Atomic Energy Agency. II. Series.

IAEAL 15–00974

FOREWORD

by Yukiya Amano
Director General

The IAEA's principal objective under its Statute is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world." Our work involves both preventing the spread of nuclear weapons and ensuring that nuclear technology is made available for peaceful purposes in areas such as health and agriculture. It is essential that all nuclear and other radioactive materials, and the facilities at which they are held, are managed in a safe manner and properly protected against criminal or intentional unauthorized acts.

Nuclear security is the responsibility of each individual State, but international cooperation is vital to support States in establishing and maintaining effective nuclear security regimes. The central role of the IAEA in facilitating such cooperation and providing assistance to States is well recognized. The IAEA's role reflects its broad membership, its mandate, its unique expertise and its long experience of providing technical assistance and specialist, practical guidance to States.

Since 2006, the IAEA has issued Nuclear Security Series publications to help States to establish effective national nuclear security regimes. These publications complement international legal instruments on nuclear security, such as the Convention on the Physical Protection of Nuclear Material and its Amendment, the International Convention for the Suppression of Acts of Nuclear Terrorism, United Nations Security Council resolutions 1373 and 1540, and the Code of Conduct on the Safety and Security of Radioactive Sources.

Guidance is developed with the active involvement of experts from IAEA Member States, which ensures that it reflects a consensus on good practices in nuclear security. The IAEA Nuclear Security Guidance Committee, established in March 2012 and made up of Member States' representatives, reviews and approves draft publications in the Nuclear Security Series as they are developed.

The IAEA will continue to work with its Member States to ensure that the benefits of peaceful nuclear technology are made available to improve the health, well-being and prosperity of people worldwide.

EDITORIAL NOTE

Guidance issued in the IAEA Nuclear Security Series is not binding on States, but States may use the guidance to assist them in meeting their obligations under international legal instruments and in discharging their responsibility for nuclear security within the State. Guidance expressed as 'should' statements is intended to present international good practices and to indicate an international consensus that it is necessary for States to take the measures recommended or equivalent alternative measures.

Security related terms are to be understood as defined in the publication in which they appear, or in the higher level guidance that the publication supports. Otherwise, words are used with their commonly understood meanings.

An appendix is considered to form an integral part of the publication. Material in an appendix has the same status as the body text. Annexes are used to provide practical examples or additional information or explanation. Annexes are not integral parts of the main text.

Although great care has been taken to maintain the accuracy of information contained in this publication, neither the IAEA nor its Member States assume any responsibility for consequences which may arise from its use.

The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1. Nuclear security focuses on the prevention of, detection of, and response to, criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities or associated activities. Other acts determined by the State to have an adverse impact on nuclear security should be dealt with appropriately. The threat of nuclear terrorism has been recognized as a matter of concern for all States, and the risk that nuclear material or other radioactive material may be used in a criminal act[1] represents a serious threat to national and international security, with potentially serious consequences for people, property and the environment.

1.2. This Implementing Guide describes the concepts and methodologies for a risk informed approach to nuclear security for nuclear and other radioactive material out of regulatory control[2], including conducting threat[3] and risk assessments that may then be used as a basis for informing the development and implementation of nuclear security systems and measures. National experience, as well as practice and guidance publications in the fields of nuclear security, threat assessment and risk management were used in the development of this publication. This publication is complementary to and consistent with the Nuclear Security Fundamentals [3] and Nuclear Security Recommendations publications:

— Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) [4];
— Nuclear Security Recommendations on Radioactive Material and Associated Facilities [5];

---

[1] Both the Convention on the Physical Protection of Nuclear Material and Amendment thereto (Article 7) [1] and the International Convention for the Suppression of Acts of Nuclear Terrorism (Article 2) [2] require States Parties to make punishable all offences that have serious consequences for people, property and the environment.

[2] The term ‘out of regulatory control’ is used to describe a situation where nuclear material or other radioactive material is present without an appropriate authorization, either because controls have failed for some reason or they never existed.

[3] In this publication, the specific term ‘nuclear security threat’ is used to refer to the meaning expressed by the definition in the Nuclear Security Fundamentals [3]. The unqualified term ‘threat’ is used more generally to refer to either the threat actor (also termed adversary) or the threat object (also termed device).

— Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control [6].

1.3. Within the scope of this Implementing Guide, 'risk' is the potential for an unwanted outcome resulting from a nuclear security event as determined by its likelihood and the associated consequences if it were to occur, including the consequences for people, property and the environment. Risk is generally a function of three components: threat, vulnerability and consequence. A risk informed approach is a prerequisite for assigning priorities and designing appropriate nuclear security systems and measures [6]. Threat and risk assessments enable a State to manage the risk and to assign priorities in allocating resources (e.g. human and financial) to organizations and to nuclear security systems and measures.

1.4. The risk informed approach is an iterative process that identifies and assesses threats and risks, and develops, evaluates and implements alternatives, and monitors and manages the resulting actions for relevance and effectiveness. This publication emphasizes the assessment of threats and risks as part of the application of a risk informed approach[4], which is consistent with international guidance [7]. A risk informed approach can help a State to allocate its resources more effectively and efficiently by systematically considering the threats and risks.

1.5. This Implementing Guide is complementary to the guidance on the development, use and maintenance of the design basis threat for nuclear material, other radioactive material, associated facilities and associated activities [8]. Further information on threat and technical information on nuclear security measures can be found in supporting guidance on combating illicit trafficking in nuclear material and other radioactive material [9].

OBJECTIVE

1.6. The objective of this publication is to provide guidance to States for developing a risk informed approach and conducting threat and risk assessments as the basis for the design and implementation of sustainable nuclear security systems and measures for the prevention of, detection of, and response to, criminal or intentional unauthorized acts involving nuclear and other radioactive

[4] The term 'risk informed approach' refers largely to the same cyclic process for managing risks understood by the term 'risk management'.

material out of regulatory control. This publication is intended to provide guidance for policy makers, law enforcement agencies and experts from the competent authorities and other relevant organizations.

SCOPE

1.7. This publication focuses on a risk informed approach and methodologies for threat and risk assessments for the development of nuclear security systems and measures for nuclear or other radioactive material that has been reported as being out of regulatory control, as well as for material that is abandoned, lost, missing or stolen, but has not been reported as such, or has been discovered by some other means.

1.8. This publication does not cover threat and risk assessment for nuclear material, other radioactive material, associated facilities or associated activities that are under regulatory control. However, it does take into consideration the potential for the material being lost, missing or stolen. Guidance for threat assessment for the theft of such material and sabotage to facilities can be found in IAEA Nuclear Security Series publications (see Refs [4, 5, 8, 10]). This publication does not cover the design and the implementation of nuclear security detection and response systems and measures (see Refs [11, 12]).

STRUCTURE

1.9. Following this introduction, Section 2 describes the basis for the management of risks from nuclear and other radioactive material out of regulatory control and, in particular, the roles and responsibilities and the legal and administrative framework for conducting threat and risk assessments, and the coordination mechanisms, both national and international, that support these activities. Section 3 provides guidance on the identification of nuclear security threats. The section describes the sources of threat (‘threats from’) and how the threat may occur. Section 4 covers the methods and procedures for the identification of targets (‘threats to’) and the estimation of potential consequences. Section 5 covers methodologies for conducting threat and risk assessments and estimating the likelihood of threats. Section 6 provides an overview of how a risk informed approach that incorporates the use of threat and risk assessments supports the process for the identification of alternative measures and implementation and management of the nuclear security systems and measures.

1.10. Following the main text, Appendices I–IV provide hypothetical, illustrative threat and risk assessments as an example of the application of risk informed approaches. These appendices are related and together form a complete example of a risk informed approach. Appendix I provides a flowchart for the complete risk informed approach including threat and risk assessments activities. Appendix II provides examples of threat assessments using two methodologies: a threat narrative approach and a threat ranking approach. Appendix III provides an example of a risk assessment approach using a probabilistic risk assessment technique. Appendix IV provides an example of the risk informed approach using results from threat and risk assessments to evaluate and prioritize activities for the design and implementation of nuclear security systems and measures. In Appendices II–IV, a common, notional 'Example State' is assumed.

2. BASIS FOR THREAT ASSESSMENT AND RISK INFORMED APPROACH

2.1. Large numbers of radioactive sources and large amounts of nuclear material and other radioactive material are used worldwide in areas such as scientific research, health, agriculture, education and industry. If such material is or falls out of regulatory control, there is the potential of it being used in criminal or intentional unauthorized acts. The potential consequences of a criminal or intentional unauthorized act involving nuclear and other radioactive material out of regulatory control depend on the material's amount, form, composition and activity. The use of an explosive with such material to make a 'device'[5] can increase the potential impact of a criminal or intentional unauthorized act involving nuclear material or other radioactive material, especially if used at a strategic location. Such acts could lead to severe health, social, psychological and economic impacts, damage to property, and political and environmental consequences. Possible acts include:

(a) The intentional dispersal of radioactive material in a public place, for example by means of a radiological dispersal device (RDD);

[5] For simplification, the term 'device' within the context of this publication is used to refer to RDDs, REDs and INDs. This is also consistent with the definition in the International Convention for the Suppression of Acts of Nuclear Terrorism [2].

(b) The placement of radioactive material in a public place, for example in the form of a radiation exposure device (RED), with the intention of irradiating people in the vicinity;
(c) The production of a nuclear explosion by an improvised nuclear device (IND).

2.2. In accordance with the relevant Nuclear Security Recommendations publication [6], the design of nuclear security systems and measures for nuclear and other radioactive material out of regulatory control should follow four steps to address the threats:

— The identification of threats;
— The identification and assessment of targets and consequences;
— The assessment of threats and risks;
— The use of a risk informed approach to prioritize nuclear security systems and measures.

2.3. The identification of threats should include consideration of potential adversaries who may contemplate using nuclear material or other radioactive material in a criminal or intentional unauthorized act to accomplish their objectives and of the potential availability to such people or organizations, both within and outside the State, of nuclear material or radioactive material suitable for such an act.

2.4. The identification and assessment of potential targets for such an act involving nuclear or other radioactive material out of regulatory control should include consideration of the attractiveness of the target to an adversary. That attractiveness may be related to the vulnerability of the target to the act or to the potential consequences of an act directed at the target.

2.5. Threat assessments should consider the motivation, intentions and capabilities of those individuals or groups who it is believed, based on an analysis of acquired data and information, might commit a criminal or intentional unauthorized act. Assessments of the potential availability of nuclear material or other radioactive material to such people, and experience from known incidents involving material out of regulatory control, are factors to be considered in a threat assessment. To ensure completeness, the assessment may include information from counterterrorism and law enforcement agencies as well as input from all agencies involved in the safety and security of nuclear material, other radioactive material, associated facilities and associated activities. The threat

assessment should also take into account the technical feasibility and historical context of the use of such material in criminal or intentional unauthorized acts.

2.6. The assessment of risk includes consideration of the likelihood of an act, in conjunction with the likelihood of success and the level of consequences, and can support the prioritization of the nuclear security systems and measures to be implemented. The process for including risk information in the prioritization of nuclear security systems and measures and for the overall management of nuclear security systems is known as the risk informed approach. International industry standards identify best practices for performing risk management [7]. These practices have been adapted for the development and prioritization of nuclear security systems and measures as part of this Implementing Guide.

NATIONAL NUCLEAR SECURITY POLICY AND STRATEGY

2.7. Effective nuclear security systems and measures for nuclear and other radioactive material out of regulatory control should be derived from a comprehensive and integrated national nuclear security policy and strategy. The national nuclear security policy and strategy should be informed by national threat and risk assessments, and should identify the competent authority responsible for conducting national nuclear security threat and risk assessments and fostering cooperation and coordination among all involved competent authorities and organizations. This policy and strategy should define the scope of, and priority assigned to, preventive measures, and detection and response measures for nuclear security, based on a graded approach. It should also include a requirement for the periodic update of threat and risk assessments in the light of new information and changing conditions, and should be reviewed and updated in accordance with the resulting changes in threat and risk assessments. The design of nuclear security systems and measures should also be based on the result of a threat assessment and the application of a risk informed approach [6].

LEGAL AND ADMINISTRATIVE FRAMEWORK

2.8. In order to develop and implement the national nuclear security policy and strategy, an appropriate legal and administrative framework should be established [6, 13]. This is particularly important for the assignment of responsibilities to competent authorities, and for the development of a

cooperation and coordination mechanism for threat and risk assessments. The framework should include:

(a) A requirement for threat and risk assessments and implementation of risk informed approaches;
(b) The assignment of roles and responsibilities for the development of threat and risk assessments for nuclear and other radioactive material out of regulatory control to a responsible competent authority;
(c) The assignment of a specific responsibility for the relevant competent authority to develop a risk informed approach and of all necessary legal and administrative authority needed to conduct such a process;
(d) A provision for full cooperation by all relevant competent authorities with the competent authority responsible for the development of threat and risk assessments for implementation of nuclear security systems and measures for nuclear and other radioactive material out of regulatory control;
(e) A provision for the competent authority responsible for the development of threat and risk assessments to update those assessments periodically and as the need arises;
(f) A provision for the competent authorities responsible for the implementation of nuclear security systems and measures to base their design of such systems and measures on the results of the risk informed approach.

ROLES AND RESPONSIBILITIES

2.9. The competent authority responsible for threat and risk assessments of nuclear and other radioactive material out of regulatory control should have in place the necessary resources and capabilities to conduct threat and risk assessments in coordination with other relevant competent authorities that make risk informed decisions within their own areas of responsibility.

2.10. The designated competent authority should ensure that all relevant data are collected and analysed, and that the threat and risk assessments are conducted by qualified and competent staff. The results of the assessments should be considered by relevant competent authorities for design and prioritization of nuclear security systems and measures. All relevant competent authorities should cooperate in the entire threat and risk assessment process to ensure that the assessment results take into account their perspectives and provide useful information to them to support their own risk informed approach.

2.11. Since the threat and risk assessments need to be kept up to date, all relevant competent authorities should provide feedback and keep the competent authority responsible for conducting threat and risk assessments up to date on all events with nuclear security implications. Because the threat and risk assessments are used to prioritize nuclear security systems and measures, the cycles of threat and risk assessments may be coordinated with budget or programmatic cycles to ensure that policy makers have access to current information and results.

COORDINATION MECHANISM

2.12. The development of threat and risk assessments relies on sensitive information derived from several competent authorities. The exchange of reliable and timely information related to nuclear security needs to be well coordinated, both nationally and internationally, in accordance with national information security policies and regulations and with international obligations. The arrangements for such an information exchange should be based on established protocols and procedures for reporting on events with nuclear security implications, such as lost, missing or stolen nuclear material and other radioactive material. The responsible competent authority for threat and risk assessments should keep all other relevant competent authorities informed of the updates of the threat and risk assessments, with regard to the need to know rule. In cases where several competent authorities are responsible for threat and risk assessments, close cooperation and coordination are particularly vital.

INTERNATIONAL COOPERATION

2.13. Effective participation in international activities may provide information and experience that can be used to improve methods and procedures for threat and risk assessments. Awareness of nuclear security events outside the State may also help to inform the understanding of the threat within a State. The IAEA Incident and Trafficking Database (ITDB) provides an international forum for up to date information on reported cases of nuclear and other radioactive material out of regulatory control, or found or detected [14]. Analysis of the data in the ITDB can provide an indication of possible threats or transboundary movements that could affect a State and of possible implications for threat and risk assessments. Such information could be of benefit to Member States for consideration in their threat and risk assessments.

2.14. Furthermore, participation in awareness and training workshops organized by international organizations and other bilateral and multilateral initiatives can be used to familiarize staff with the latest methodologies and procedures, and to help in acquiring expertise and competence. Assistance on matters related to threat assessment may be facilitated by relevant international organizations or may be requested directly on a bilateral or multilateral basis.

3. IDENTIFICATION OF NUCLEAR SECURITY THREATS

3.1. Threats may be identified in terms of 'threats from' and 'threats to'. Identification of 'threats from' is based on consideration of who the adversary is, which type of nuclear material or other radioactive material the adversary might have or seek access to, and how the adversary might seek to cause harm through that material. In the context of nuclear and other radioactive material out of regulatory control, where the adversary may have possession of the material, the 'how' will typically be a question of the type of device the adversary might seek to use. Identification of 'threats to' considers the strategic locations where nuclear or other radioactive material out of regulatory control may be used. Specific components that may be considered for a threat assessment are summarized in Fig. 1. States may also consider additional components as appropriate for the State.

3.2. The WHO/WHY component identifies and describes the adversaries who may attempt criminal or intentional unauthorized acts. Potential adversaries should be analysed to identify their motivation[6], intention and capability. This should include consideration of adversaries who might attempt criminal or intentional unauthorized acts within the State that would affect another State. Adversaries should be evaluated based on the likelihood of their attempting particular acts, their ability to obtain the financing and technical capabilities necessary to acquire

[6] Motivation may be a useful consideration in identifying potential adversaries and the types of criminal or other unauthorized act they might attempt (e.g. adversaries' motivations may influence their choice of target). However, whereas nuclear security measures may seek to influence the intentions and capabilities of adversaries, such measures do not attempt to influence their motivation. Therefore, while considerations of motivation may play a role in threat identification, they may be less relevant to other aspects of threat assessment or to the design and implementation of nuclear security systems and measures.

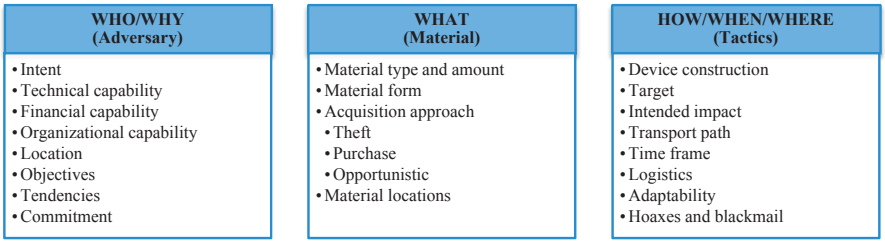


FIG. 1. Components of threats.

the material and construct a device, and their knowledge of the information required to successfully attempt the act. Paragraphs 3.18–3.23 describe methods and processes for analysing adversaries in greater detail.

3.3. The WHAT component identifies the material that may be used by an adversary. If a State has a small number of locations in which nuclear material and other radioactive material are stored or used, the associated facilities and associated activities may be evaluated individually. If a State has many facilities and activities, these may be evaluated as groups of similar types or individually, depending on the desired level of detail for the assessment. In addition to such facilities and activities, the possibility of material being acquired outside the State, or following its illicit trafficking, should be considered. The different possibilities could include the different types of material that may be acquired, the different types of site where the material is stored or used, and the methods an adversary may choose to acquire the material or smuggle it into, or out of, the State. The likelihood of choosing a particular facility or material should be estimated based on knowledge of the adversary's general preferences, the accessibility of the material or the type of device that might be favoured by the adversary. The likelihood of acquiring material depends on the capability of the adversary and the vulnerability of the material. Often, information from existing vulnerability assessments may be used to assess the likelihood of acquisition of material by the adversary. Paragraphs 3.6–3.9 describe how to assess the possibility of material being acquired from the State's associated facilities and associated activities. Paragraphs 3.10–3.17 describe the vulnerabilities that might apply to material out of regulatory control within the State and to material that crosses the State's boundaries.

3.4. The HOW/WHEN/WHERE component describes the characteristics of the particular tactic. For example, assuming that an adversary has acquired material, there are two key steps that the adversary may need to take in constructing

a device. The first is adapting it into a device or processing the material to change its form so that it is usable in a device. The second step is the design and construction of the device. Different designs and different levels of skill in constructing devices may result in devices with different levels of effectiveness. More complicated designs may need more time, more people and more complex infrastructure to develop (e.g. specialized tools or a safe place to work), whereas less sophisticated designs may be constructed more quickly and reliably, without the need for specialized equipment. The result of the analysis is an estimate of the likelihood of the existence of devices of different effectiveness depending on the assumptions related to material acquired and the adversary's capability. Other scenarios such as trafficking do not necessarily involve devices and may either be treated as part of a larger adversary scenario involving a device or as a separate act in itself. A completed device will usually need to be transported to the target where it will be deployed. Consideration therefore needs to be given to both the ultimate target (which in turn influences the level of consequences) and the transport route. The likelihood of the adversaries being intercepted prior to deployment of the device can be estimated by considering the opportunities for detection using instrument alarms, information alerts or other regular law enforcement activities and awareness as part of a State's nuclear security detection architecture [11]. More detailed guidance on assessing how, when and where is provided in paras 4.3–4.6. In assessing the deployment of a device, it is important to consider its effectiveness and the potential consequences. Impacts should be assessed both in terms of intended effects and the likely actual effects. More detailed guidance on assessing the consequences of an action with nuclear security implications is provided in paras 4.7–4.18.

3.5. A threat assessment is an attempt to characterize and, if possible, quantify threats through the process of identifying or evaluating adversaries or actions that have the potential to harm persons, property, society or the environment. Threat assessment is generally based on an evaluation of the intent and capability of adversaries, where intent is often estimated as a frequency (e.g. how many attempts per year) and capability is a likelihood of success given an attempt. Three typical approaches, which may be used in combination, are described below:

(a) Measures of threat may be estimated qualitatively, simply as low, medium or high (or a scale like that in Table 1, in Section 4), or with more sophisticated scales using qualitative descriptors or qualifiers to describe threat ratings, sometimes referred to as a 'word ladder'. This most basic form of qualitative threat assessment is necessarily based on the elicitation of expert judgement.

(b) Measures of threat may be estimated quantitatively from expert analysis and empirical data. If such quantitative estimates are used, it may be very difficult to estimate the likelihood values, and therefore it is also important to estimate the uncertainty in each estimate of likelihood.

(c) For security applications, likelihoods associated with threats are often not estimated at all. Rather, security measures are assessed against a specific real or hypothetical adversary with a defined capability. This approach is called a design basis threat (DBT), since the identified capability effectively determines performance specifications for the design of the security systems and measures. The process for the development of a DBT for a nuclear facility is described in Development, Use and Maintenance of the Design Basis Threat [8]. A similar process may be used for other nuclear security applications (e.g. nuclear security measures for a major public event).

VULNERABILITY OF NUCLEAR AND OTHER RADIOACTIVE MATERIAL UNDER REGULATORY CONTROL

3.6. In order to carry out a criminal or intentional unauthorized act involving nuclear material or other radioactive material, an adversary must acquire the material.[7] An adversary may attempt to acquire material from existing facilities and activities, from others who have material that is already out of regulatory control or from outside the State. As part of the threat assessment, it is important to estimate the likelihood that material under regulatory control may fall out of regulatory control. The ITDB indicates that material may be lost or missing from regulatory control worldwide through theft, accidental loss and disposal without authorization [14].

3.7. One method for estimating the likelihood of material under regulatory control falling out of regulatory control is to compare the capabilities of identified adversaries with the vulnerability of associated facilities and associated activities that hold such material.

[7] As outlined in para. 1.9, the scope of this Implementing Guide is nuclear and other radioactive material out of regulatory control, and therefore criminal or intentional unauthorized acts directed at nuclear material, other radioactive material or their associated facilities and associated activities (i.e. acts of sabotage) are outside the scope of this publication.

3.8. Operators of associated facilities or associated activities may already have completed vulnerability assessments against a DBT or an alternative threat assessment, and therefore may have an understanding of the performance of their nuclear security systems and measures against that specific threat. The DBT should be defined such that the likelihood of a well designed nuclear security system failing to prevent an adversary with capability equal to, or less than, that of the DBT from successfully removing material is very low. However, vulnerability should be assessed for all relevant facilities and activities, some of which may not themselves have conducted vulnerability assessments. Furthermore, if adversaries are identified that have capability greater than or qualitatively different from that of the DBT, additional assessment similar to that performed for the DBT may be needed to estimate such an adversary's probability of success. Consideration should be given to several alternative methods for acquiring material from a facility or activity (including during transport), such as armed assault, insider assistance, falsified accounting of material and theft.

3.9. Adversaries are likely to seek out facilities or activities where the material is more vulnerable. Thus, the likelihood of an adversary acquiring material may be approximately equal to the likelihood of acquiring the material from the most vulnerable site. Similarly, the likelihood that a particular facility or transport route may be selected by an adversary for acquiring material is related to the vulnerability of the facility or transport route. More vulnerable sites are more likely to be selected. In this manner, a change in the vulnerability of any site also results in a change in threat. This has implications for the analysis of alternatives. When a change is made in the nuclear security systems and measures at a location, the vulnerability of the material there may change and therefore the threat may also change, potentially both in magnitude and in the specific scenarios that are most likely.

AVAILABILITY OF NUCLEAR AND OTHER RADIOACTIVE MATERIAL OUT OF REGULATORY CONTROL

3.10. Adversaries might also seek to acquire nuclear and other radioactive material that is already out of regulatory control. Radioactive material is present in almost all countries, under various levels of security. Some nuclear material may not be properly accounted for, and some radioactive sources may not be properly registered [5]. Some abandoned, lost, missing or stolen nuclear and other radioactive material may not have been reported as being out of regulatory control.

3.11. From 1993 to the end of 2012, the ITDB received well over 2000 reports of instances of nuclear and other radioactive material out of regulatory control [14]. Reports of material out of regulatory control should be taken into account in a threat assessment. Unauthorized individuals have been known to offer nuclear material and other radioactive material for sale, and others have attempted to purchase nuclear material and other radioactive material, apparently for use in a criminal act. While many offers to supply such material have transpired to be fraudulent, there may be cases involving actual acquisition by adversaries of nuclear and other radioactive material out of regulatory control that have not been detected.

3.12. Radioactive sources out of regulatory control may simply be discovered by adversaries or offered for sale to adversaries. These possibilities should be considered when estimating the likelihood of an adversary acquiring material out of regulatory control.[8] Even less likely, an adversary might also purchase or otherwise acquire a completed device containing material that is already out of regulatory control, and this possibility should also be considered in threat assessments.

3.13. Hence, the threat assessment should include estimates of the likelihood of an adversary being able to acquire material already out of regulatory control, both within and outside the State, and descriptions of the types of material that may be acquired. Estimating this likelihood may necessitate the competent authority identifying all of the locations where material has been created, used, stored or transported. The competent authority also needs to understand the common uses of nuclear material and other radioactive material within the State and its history of material control and accounting for nuclear material and of radioactive source registers and other mechanisms for other radioactive material. A likelihood may be assigned to an adversary obtaining nuclear or other radioactive material that is lost, missing or stolen. Since records of such cases may, by definition, be incomplete or inaccurate, this likelihood will be more difficult to determine, and therefore appropriate uncertainty bounds may also need to be estimated.

[8] There could also be instances in which the nuclear or other radioactive material out of regulatory control is transported without the knowledge of the carrier or shipper.

TRANSBOUNDARY MOVEMENTS

3.14. The ITDB shows that transboundary movements of nuclear and other radioactive material out of regulatory control occur. Consequently, the likelihood of nuclear or other radioactive material out of regulatory control being acquired by an adversary will depend upon the availability of such material anywhere, not just within the State.

3.15. Assessing the threat arising from material already out of regulatory control is therefore difficult, since the State may not have a detailed understanding of the likelihood of material being available in other States. Data from the ITDB may be used to provide a conservative estimate on the amount of material available. However, the amount of material out of regulatory control that has not been reported to the ITDB is unknown. The competent authority will need to decide what weight to give to this factor when assessing the threat.

3.16. As part of its national level threat assessment, the responsible competent authority should consider, in addition to the types and amounts of material out of regulatory control, the transit routes into and out of the State by which such material could be moved. The competent authority should therefore consider nuclear or other radioactive material:

(a) Entering or exiting the State via designated points of entry (land, air or water), in commercial traffic or in privately owned vehicles;
(b) Entering or exiting the State via undesignated points of entry;
(c) Passing through the State in transit (i.e. entering the State but not intended for final delivery within the State). In many cases, such material is not identified and does not necessarily comply with the State's internal control procedures.

3.17. The competent authority should consider the possibility of an adversary exploiting the global supply chain to transport illicitly nuclear and other radioactive material out of regulatory control. Implementing effective border monitoring systems and measures as part of the nuclear security detection architecture may serve to deter, detect or prevent transboundary movements of such material and may reduce the risk considerably [11]. The effectiveness of the State's procedures and capabilities, as well as an adversary's awareness of them, will affect the level of threat assessed from material acquired outside the State.

ANALYSIS OF ADVERSARY CAPABILITY AND INTENT

3.18. Paragraphs 3.10–3.17 focus on assessing the availability of nuclear and other radioactive material out of regulatory control that may be used in a criminal or intentional unauthorized act. The likelihood of such material being used in an act depends greatly on the potential adversaries. This subsection focuses on evaluating the adversaries by assessing their capabilities (e.g. technical or financial) and their intentions (particularly whether they would be likely to use the nuclear material or other radioactive material and if so, how they might use it and their likely attitude to radiological and other risks to themselves). Assessing adversaries is a dynamic process. Reliable and up to date information about the capability and intent of an adversary may be difficult to acquire, and the information that is available may be contradictory and uncertain. The difficulty is in part due to adversaries' measures to conceal their activities. Furthermore, adversaries adapt to changing circumstances, and changes in the defensive posture of the State (such as increased security at a particular site) will typically result in changes in the likelihood of a particular adversary committing a particular act. These changes do not necessarily decrease or increase the overall likelihood; the changes may only shift the adversary's attention to other targets or other kinds of act. The likelihood estimates for different types of act should be dynamic, with relative likelihoods shifting as the State's nuclear security regime improves.

3.19. The first step in assessing adversaries is identifying the potential adversaries (as shown in the "Adversary" column of Fig. 1). The competent authority responsible for threat and risk assessments should work closely with law enforcement and State intelligence authorities to gain insight into the information a State has on a particular adversary. Information may also be available to a State via bilateral or multilateral agreements or from international law enforcement organizations. There are many possible motivations for criminal or intentional unauthorized acts, and many potential adversaries. Where adversaries can be identified as individuals or specific groups, this will allow for more accurate and specific characterization of their intentions and capabilities. Alternatively, or in addition, specifying types of individual or group as a category may allow more efficient analysis and may allow the analysis to take some account of adversaries that are not yet known.

3.20. Identified adversaries should be characterized based on their likely intentions. Specific intentions are often strongly influenced by the general motivation of the adversary. Motivations may have financial, political, ideological or personal aspects. Key elements of this characterization are:

(a) Would the adversary be willing to deploy nuclear or other radioactive material out of regulatory control in a criminal or intentional unauthorized act?
(b) Does the adversary intend to commit an act within the State?
(c) Does the adversary intend to use the State as a staging area for an act in or against another State?

3.21. The likelihoods of an adversary attempting different types of criminal or intentional unauthorized act may be assessed quantitatively (ideally a probability distribution), but assessments may be qualitative if necessary (e.g. low, medium or high likelihood). In all cases, the uncertainty in the estimate should be understood and used in the overall threat assessment.

3.22. In addition to assessing the possible intentions of an adversary to commit a criminal or intentional unauthorized act using nuclear or other radioactive material out of regulatory control, the adversary's capability to commit such an act successfully should be assessed. Discussion of capability is often divided into two categories: organizational capability and logistics. An adversary would need to acquire either material that is already out of regulatory control or material that is under regulatory control from where it is being used, stored or transported. Both options are likely to need significant resources of some kind; for example, access to material out of regulatory control may be relatively easy if sufficient financial resources are available, whereas access to material under regulatory control may need more technical or human resources. Once material has been acquired, creating a device also needs infrastructure and specialized expertise. Such capabilities are often tightly controlled and monitored in parallel with the security of the material, and may be difficult for an adversary to acquire. The competent authority should assess the likelihood that such capability is available within the State or can be acquired outside the State and transferred into it.

3.23. The task of the competent authority in assessing the intent and capability of adversaries is complicated by the lack of historical data to use in estimating likelihood. The competent authority may estimate the intent and capability based on an adversary's statements, evidence of activity that may have been undertaken in support of committing a criminal or intentional unauthorized act, and knowledge of an adversary's objectives and preferences. Such information about adversaries may be considered sensitive, and it should be protected in accordance with national policy on information security. While estimates of likelihood may be highly uncertain when based on such data, they nevertheless can provide relative indications of the threat from different adversaries or types of adversary.

4. IDENTIFICATION AND ASSESSMENT OF TARGETS AND POTENTIAL CONSEQUENCES

4.1. Section 3 focuses on identifying threats, including the adversaries and the means for carrying out a criminal or intentional unauthorized act (nuclear or other radioactive material out of regulatory control used in devices). This section provides guidance on methods and approaches for identification and assessment of targets and potential consequences of a nuclear security event involving nuclear and other radioactive material out of regulatory control. To complete the overall risk assessment, it is necessary to understand the attractiveness of different targets and the likely consequences of different devices being deployed against those targets, since the likelihood of an adversary attempting an act against a target depends on the value of that particular approach to that particular adversary.

4.2. In Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control [6], 'target' is defined as nuclear material, other radioactive material, associated facilities, associated activities or other locations or objects of potential exploitation by a nuclear security threat, including major public events, strategic locations, sensitive information and sensitive information assets. Since this Implementing Guide focuses on nuclear and other radioactive material out of regulatory control, the scope of the term 'target' within the context of this publication does not include material under regulatory control or associated facilities and associated activities.

IDENTIFICATION OF TARGETS

4.3. Targets may be identified very specifically (e.g. a specific building, monument or event) or as a class (e.g. office buildings, monuments, sporting events, or locations in a specific city). For a general threat assessment in the absence of specific intelligence, identifying specific targets will result in a larger target list (which must then be prioritized) than identifying target classes. Sometimes a mixture of specific targets and classes of target is appropriate if there are specific places within some classes that are much more obvious or more likely than others in the same class. Considering the difficulty of acquiring nuclear material or other radioactive material and the relative rarity of devices containing such material, it may be appropriate to limit the target list to the highest value (e.g. high likelihood of success and high impact) targets available rather than all potential targets.

4.4. When identifying targets, the consequences for people, property and the environment may be considered in the following classes:

(a) Buildings, monuments or places of symbolic importance: Such sites may include government buildings, important private institutions, monuments, palaces, museums, religious sites, or sites of great cultural heritage value or political significance. They may also be of value due to their affiliation with another State (e.g. embassy or consulate).
(b) Critical infrastructure: Such sites may include critical nodes for power, water, natural resources, transport or communications. Dams, power plants, refineries, water treatment plants, bridges, or other facilities and information systems or structures that provide necessary services to large numbers of people may be attractive potential targets.
(c) Population centres: Areas of dense population may be attractive to adversaries intending to cause injury, death or major disruption. Concentrations of particular groups of people (e.g. ethnic or religious groups) may also be targeted.
(d) Special events may combine aspects of particular symbolism with large numbers of people in a small area and may be attractive to adversaries. Such events as major sporting competitions, political rallies, national celebrations or religious festivals may be included in this class of targets.
(e) Environmental resources or ecosystems.

4.5. Identified targets may be prioritized based on the estimated likelihood of being chosen, on their attractiveness to the adversary or on the potential consequences of an attack. The competent authority should recognize that different adversaries may prefer different targets, depending on their objectives and capabilities. In addition, some targets may be more attractive for some types of nuclear security event than others. The relative attractiveness of different targets will depend upon adversary objectives, and is commonly related to the desired impacts, including:

(a) The population affected — who and how many;
(b) The financial impact of disruption and damage;
(c) The economic or logistical importance of the target;
(d) The symbolic value of the target.

4.6. Attractiveness may also depend upon the vulnerability of the target (i.e. the ease with which it can be attacked, the ease of escape and the likelihood of success). Thus, assessment of target attractiveness is closely tied to the assessment of the vulnerability of the target and of the potential consequences

of a nuclear security event. The relative attractiveness of targets may vary over time with changes in target defences or adversary objectives.

CONSEQUENCES OF NUCLEAR SECURITY EVENTS

4.7. The consequences of a nuclear security event will depend on the nature, location and other circumstances of the event. Consequences may escalate from initial direct effects to follow-on secondary and tertiary effects.[9] For criminal or intentional unauthorized acts involving nuclear material and other radioactive material, the potential consequences for people (generally health or societal impacts), property (generally economic impacts) and the environment should be assessed. Potential consequences must be understood in order to conduct a threat assessment, and should be evaluated in some detail when performing a risk assessment. Paragraphs 4.7–4.18 focus on the estimation of such consequences.

4.8. For nuclear security events, potential consequences for human health should be estimated as part of the risk assessment. These may include casualties (deaths and injuries) caused by the device (e.g. resulting from an explosion) as well as exposure to radiation or intakes of radionuclides from the nuclear material or other radioactive material, which could lead to death, serious injury or significant impairment of the function of tissue or an organ. In the case of an IND, there may be radiation induced effects from the nuclear explosion as well as non-radiological effects from the blast and heat from the explosion, and longer term radiological effects associated with fallout.

4.9. Economic costs may arise from many aspects of a nuclear security event, but particularly from addressing impacts on people, property and the environment. These may include costs of treating those who become ill (or who are worried that they have become ill), of decontaminating affected areas (or of removing and disposing of soil, buildings and contents that cannot easily be decontaminated), and of evacuation, relocation, and business disruption and recovery. In addition to the direct costs of an event, there may also be indirect effects on a State's economy.

---

[9] Secondary and tertiary effects are consequences that occur as a result of a nuclear security event but are not direct effects of the attack. For example, detonation of an RDD at a port may have direct effects, such as injuries to people and damage to property, but may also lead to the closure of the port during investigation and remediation work, resulting in a reduction in trade and possibly the closure of businesses that depend on the port. These additional consequences are secondary and tertiary effects, respectively.

4.10. Environmental consequences may also arise from a nuclear security event. Radioactive material may be intentionally used to contaminate, for example, soil, groundwater or fragile ecological areas, which might not readily be decontaminated, or dispersed radionuclides from a device may find their way into the environment. Contamination of an area may result in its permanent abandonment by inhabitants and avoidance of agricultural produce and other industrial products from the area. The long half-life of some radionuclides means that the impact of contamination may persist for long periods of time.

4.11. Lastly, there may be societal consequences for a State, a region or the world from a criminal or intentional unauthorized act. There may be an outburst of outrage or anxiety from the individuals or communities affected. At a local level, areas may be evacuated and later avoided. At a national level, the political process (e.g. elections) might be interrupted or influenced. Societal consequences may also extend beyond the State in which the event occurs, for example through disruption of supply chains, large scale movement of people or diplomatic complications. These consequences are extremely difficult to predict or quantify and, in many cases, the extent of the consequences depends as much on the authorities' response to the act as the act itself. Great caution is therefore needed in attempting to estimate such consequences.[10]

4.12. Consequences can be estimated in several ways, including by qualitative ranking or by detailed consequence modelling.

4.13. Qualitative ranking of consequences involves subject matter experts ranking the potential consequences in categories based on qualitative descriptions such as 'severe', 'moderate' and 'minimal'. An example of a consequence matrix, with four different types of effect and five categories for ranking, is shown in Table 1.

4.14. The qualitative ranking method commonly uses broad categories to describe the consequences of a nuclear security event for people, property and the environment. The magnitude of consequences represented by these categories may vary by orders of magnitude (e.g. as in the health impact row in Table 1). The aim should be to create categories broad enough to help subject matter

[10] It may also be worth noting that the four categories of consequence described — health, economic, environmental and societal — are not mutually exclusive. Consequences in one category may have a direct impact on the consequences in another category. For example, concern among people living near the site of an explosion (a societal consequence) due to radioactive contamination from the explosion (an environmental consequence) may lead to abandonment of the area and a drop in commercial activity (an economic impact).

TABLE 1. EXAMPLE OF A QUALITATIVE CONSEQUENCE MATRIX

Impact elements	1	2	3	4	5
Health impact	Likely to produce no casualties	Likely to cause fewer than ten casualties	Likely to cause more than ten casualties	Likely to cause more than 100 casualties	Likely to cause more than 1000 casualties
Economic impact	Costs equal to replacement of a building	Costs significant at the city district level	Costs significant at the city level	Costs between 1% and 10% of GDP[a]	Costs in excess of 10% of GDP[a]
Environmental impact	No significant contamination	Small area or temporary contamination	Significant contamination in a small area	Large area with measurable contamination or small area with critical resources unavailable	Large area with critical resources unavailable owing to contamination
Societal impact	No major change in population behaviour or effects on social functioning locally or nationally	Occasional or minor loss of non-essential social functions in a circumscribed geographical area	Loss of many non-essential social functions in a circumscribed geographical area	Dysfunctional behaviour and disruption of important social functions for a sustained period	Loss of belief in government and institutions Widespread disregard for official instructions Widespread looting and civil unrest

Note: The numbers and descriptions are indicative only and would need to be adapted to national circumstances and priorities.

[a] GDP: gross domestic product.

experts to select the correct category to describe the consequences of the event, while maintaining meaningful distinctions between the different categories. Thus, categories of the right breadth can allow for the uncertainty in estimates of consequence, while ensuring that cases can reliably be placed in the correct category. The definitions of categories may include quantitative measures of some types of consequence, such as health, economic and environmental impacts, whereas other categories, such as societal consequences, are likely to be definable only in qualitative terms. This approach allows disparate elements of impact to be evaluated in a common framework. However, care should be taken in developing categories to ensure that impacts described by the same qualitative terms are of comparable magnitude for each type of impact. This is known as calibration of scales across types. It is also important to ensure that categories on the rating scale reflect all levels of impact: a common mistake is to set the highest category at too low a level so that extreme impacts are indistinguishable from major impacts.

4.15. Detailed consequence modelling attempts to model the effects of an adversary's chosen action (e.g. device deployment) on a target location. Estimates of factors such as explosive effects, dispersal of radioactive material, distribution of individual and collective doses to the population, and levels and extent of contamination, among others, are determined using mathematical models of the event rather than subjective estimates. These models may be very simple (e.g. a blast radius and uniform dispersal over an affected quadrant based on wind direction) or very detailed (e.g. computational fluid dynamic models of airflow), and should, where possible, be based on empirical data. In practice, even when detailed models are used, there is usually substantial uncertainty in estimates of the level of consequences because of unpredictable factors (such as wind speed and direction), so estimates will typically have relatively wide error bars.

4.16. Common endpoints of consequence assessments include the number of casualties and the economic cost of a nuclear security event. Sometimes, the number of casualties and the economic cost of the nuclear security event are combined by applying a nominal monetary value to each casualty (e.g. the value of a statistical life[11]) and adding the result to the economic cost.

[11] The concept of the value of a statistical life is intended to represent the amount that people would be willing to pay to reduce risk so that, on average, one person fewer is expected to die from the source of the risk.

4.17. Evaluating societal consequences presents a difficult challenge. While it is clearly important to incorporate the effects on society in any assessment of consequences — and, in practice, societal effects may be the principal consequences intended by the adversary and the most important for the State — societal consequences are extremely difficult to estimate, even qualitatively. Furthermore, societal consequences may be dramatically influenced by the State's response to the nuclear security event and, thus, are not completely determined by the event itself. There is no generally accepted method for estimating societal consequences. Therefore, States will need to identify their own approaches for incorporating societal effects into consequence assessments.

4.18. Since consequences are a function of the radioactive material used, the characteristics of the device, the characteristics of the target, the effectiveness of the response, and the people, property and the environment near the target, consequence estimates can span a broad range. It may therefore be sufficient to use order of magnitude estimates of consequences to distinguish between different scenarios. For simple analyses, consequences may be estimated as levels (e.g. 1 to 5 or qualitative category descriptions, as in Table 1) and a number representing a central estimate of economic impact may be used for numerical calculations. Alternatively, all units may be removed from the consequence estimates and a 'normalized impact rating' may be used to indicate relative consequences. The normalized impact rating is used to demonstrate relative impact levels without referring to specific monetary amounts.

5. THREAT AND RISK ASSESSMENTS METHODOLOGIES

5.1. In Sections 3 and 4, the components of threat and risk assessments are described. In this section, common methods for assembling those components into useful assessments are described. Figure 2 shows the components of threat and risk and their relationship to each other. In this usage, threat typically comprises intention and capability, and is informed by the potential consequences and likelihood of success (from the adversary's perspective) of the particular type of nuclear security event. Risk is a function of threat, vulnerability and consequences, and may be expressed quantitatively — for example as an expected loss (consequence per year) — or qualitatively using relative rankings (e.g. low, medium and high). Since estimating risk depends on estimating threat, vulnerability and consequences, the threat assessment is typically completed before, and informs, the risk assessment.

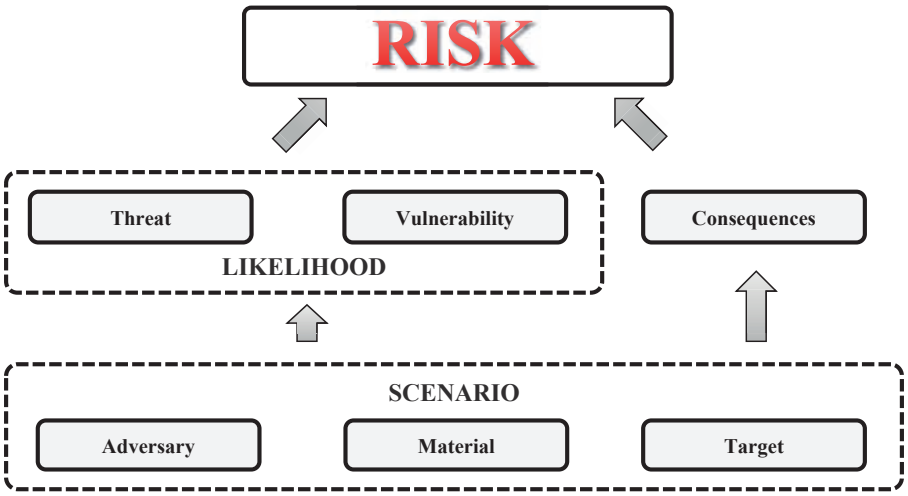


FIG. 2. Relationship between threat and risk and supporting components.

5.2. There are many types of threat and risk assessment and many methodologies appropriate for a variety of situations. The particular methodology chosen should be tailored to the specific situations that are being assessed and to the available resources and technical capabilities. One important decision is whether the assessments should be essentially qualitative or quantitative. Generally, if a qualitative (e.g. low, medium and high) assessment is sufficient to inform prioritization decisions, then qualitative methods should be used. If, however, there is a need for more refined characterization of threat or risk, or greater discrimination between different threats or risks, a more quantitative methodology should be selected.

5.3. There are also different levels of focus for threat and risk assessments, the two most common being strategic and tactical. Strategic assessments consider longer timescales and are focused on managing resources and developing plans for improving capabilities. Tactical assessments are typically performed under significant time constraints and are used to inform operational decisions in specific cases. Since this publication is focused on threat and risk assessments to support the design and implementation of nuclear security measures, the assessments described here are strategic.

5.4. Threat assessment for nuclear security differs from other threat assessments for several reasons. For example, the technical and scientific characteristics of nuclear material and other radioactive material are a significant factor in the nature and level of the threat as compared to more conventional weapons, such as firearms and explosives. Furthermore, the availability and potential use of nuclear material and other radioactive material is the defining aspect of the threat assessment, which implies a narrower and more specific scope compared to, say, a criminal or intentional unauthorized act that depends on the acquisition of a firearm. Furthermore, the limited number of cases of nuclear security events means that the empirical basis for accurately assessing both threat and risk is limited.

THREAT ASSESSMENT METHODOLOGIES

5.5. There are a number of techniques used to perform threat assessments. Two common methodologies are:

(a) The threat narrative approach: A qualitative method for describing threat level and characteristics;
(b) The threat ranking approach: A semiquantitative method for estimating threat components and combining them into an overall threat assessment.

These methodologies may be used alone or in combination. The threat narrative approach results in a threat description which may be effectively used to assess a threat level and to support a qualitative risk assessment methodology. Since it does not provide quantitative estimates, it is inappropriate for use with a quantitative risk assessment methodology unless supplemented with an approach that provides quantification. The threat ranking approach may be used with either qualitative or quantitative risk assessment methodologies, since the rankings may be readily converted into relative likelihood estimates.

5.6. In both cases, the methodologies follow a common, three stage analysis cycle for assessment, similar to that presented in Fig. 3. The first step in the cycle involves the competent authority planning the threat assessment, collecting new or existing sources of threat information, evaluating the quality and credibility of the information, and correlating information that relates to the same threats, events or activities. The second step is the analysis, in which the information is integrated and interpreted to form a cohesive body of knowledge. In the last step of threat assessment, the competent authority responsible for the threat

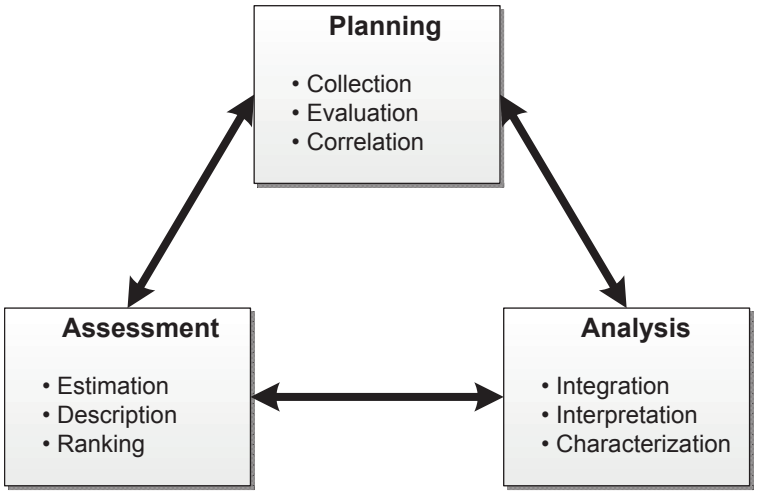


FIG. 3. Threat assessment process showing key activities.

assessment assesses the relative level or likelihood of the threats considered in the assessment and develops the threat narrative or threat ranking.

Threat narrative approach

5.7. The threat narrative approach provides a qualitative measure of threat. Subject matter experts prepare a detailed profile of the intentions, capabilities and motivations of adversaries. The threat assessments provide an understanding of the organization, capabilities, operations and support mechanisms of adversaries. This information is useful in evaluating for different adversaries the likely types of action, targets and means of carrying out the action.

5.8. The threat narrative approach uses a set of standard techniques focused on the development of hypotheses, reconstructing the course of individual nuclear security events, identifying a series of related nuclear security events, understanding adversary networks and analysing the scope of, and patterns in, related activity. It allows the analyst to include subtle assessments and statements to reflect uncertainty and unpredictability and to augment incomplete information [15].

5.9. The threat narrative approach comprises two main techniques: analysis of nuclear security events and analysis of specific adversary characteristics. The analysis of nuclear security events looks for trends and indicators of preferences in known nuclear security events. Events may be examined with respect

to the type of radioactive material involved, the location of the incident, the level of capability of the adversary and the nature of the adversary's action. The analysis of specific adversary characteristics includes consideration of the adversaries' intentions, capabilities, organizations and financial resources, and their past activities, preferences and tendencies.

5.10. Techniques that support these analyses include using geographic information systems to show the relationship between locations of adversaries, nuclear security events and related activities, database structures for understanding such relationships, and charts of linkages between individuals and groups (e.g. social network analysis tools). Examples of some of these techniques can be found in Appendix II.

5.11. The results of a threat narrative approach are descriptions of specific adversary characteristics and tendencies. An example is shown in Table 2 for a set of notional adversaries.

Threat ranking approach

5.12. The threat ranking approach provides a way to assess threat quantitatively. The method combines the estimation of relative likelihoods of threats with narrative descriptions of types of threat, using a combination of rating scales with qualitative descriptors, also known as 'word ladders'. It uses a similar approach to developing an overall understanding of the threat to that in the threat narrative approach, but the assessment phase of threat ranking is focused on estimating the relative likelihoods of different aspects of the threat. These aspects typically include capability and intention, and may include other aspects of the nuclear security event, such as types of material, types of device or types of target. The results of assessing these aspects of the threat are then combined into an overall 'threat score', using a predefined technique. The technique used for combining rankings for different aspects of the threat must be mathematically sound. It is important to note that for a quantitative threat assessment specific to nuclear security, the scales for evaluating different threats (or aspects of threat) are likely to be calibrated relative to one another but not in relation to any other type of threat. Thus, a nuclear security related threat rated as "high" might be low relative to that for other types of attack, such as those involving explosives and firearms. For an all hazards assessment, on the other hand, nuclear security related threats are assessed alongside other threats.

TABLE 2. EXAMPLE THREAT ASSESSMENT RESULTS IN NARRATIVE FORM

Threat	Intention	Capability
Group A	If Group A possessed material, they would be likely to use it in an RDD in order to contaminate an urban area and inflict a high economic cost. However, they are unlikely to engage in any activities that will result in large numbers of casualties.	Group A has contacts with drug trafficking groups and organized crime, and, with these contacts or alone, may be able to acquire radioactive material.
Group B	Group B does not seek to cause mass casualties, but they are known to carry out targeted attacks. Targeted contamination of food or water supplies would be consistent with its typical tactics.	Group B has contacts with smuggling groups and organized crime, and, with these contacts or alone, may be able to acquire radioactive material.
Group C	Group C is interested in almost any attack that will result in substantial disruption, destruction or mass casualties. They have conducted these types of attack in the past, and were responsible for a number of planned attacks that were thwarted. They are interested in acquiring radioactive material to use in an RDD. If they could acquire the material and construct an IND, or acquire an already constructed nuclear device, they would detonate it in an urban population centre.	Limited contacts with organized crime and smugglers reduce Group C's ability to obtain material or devices via traffickers. The group has substantial resources to pose a significant threat of direct theft of material from a regulated facility or activity.

Note: All descriptions are hypothetical. IND — improvised nuclear device; RDD — radiological dispersal device.

5.13. The rating process is the most critical element of the threat ranking approach. The process should follow good practice for the elicitation of data from subject matter experts and should include well defined meanings for the different ratings. The attributes (criteria, factors or categories) that are rated should be orthogonal, meaning that they should not overlap in such a way as to cause double counting of aspects of the threat. Separate evaluation scales are usually described for each attribute that is to be rated. For example, there may be separate scales for 'financial resources' and 'technical capabilities', and these should then be rated independently. A good practice is to use descriptive text to explain each level on the scale. Scales with five, seven or ten levels are common and provide differentiation without making the assessment process overly complex,

but the number of levels is not itself an indicator of accuracy or precision, since the uncertainty in the judgements will remain. Documenting the uncertainty or confidence for each rating remains an important aspect of the assessment.

5.14. The ratings of an adversary with respect to each attribute are combined into an overall rating for each adversary, providing a picture of the overall threat. There are many different approaches that may be used for combining ratings, depending on the particular rating approaches. Among the most common are:

(a) Highest rating: The highest rating from any attribute is applied to provide the overall threat rating for that adversary. This approach provides conservative threat assessments and reflects a belief that adversaries will seek to reduce their weaknesses, so their attribute ratings in lower scoring areas may be expected to increase.
(b) Average rating: Scores from the different attributes are averaged, often by applying numerical values (e.g. on a 1–5 scale) to the individual estimates and taking the mean value. This approach gives equal weight to each of the attributes. The value closest to the average is used for the overall threat score. This approach tends to reduce the effects of very high or very low ratings on particular attributes, which in fact might merit closer study.
(c) Lowest rating: The lowest rating from any attribute is applied to provide the overall threat rating for the adversary. This approach assumes that the lowest rating represents the most demanding obstacle that the adversary would have to overcome, and reflects a belief that an adversary cannot be successful without overcoming that obstacle.
(d) Convert to likelihood: The scores are converted to likelihood values for each attribute (e.g. motivation, capability and intent), often with uncertainty bounds, which are multiplied together to obtain an overall likelihood for the adversary. Particular care is needed when using such an approach to ensure that the likelihood values can be specified well enough to provide meaningful distinctions between threats. For example, some assessments may need to distinguish among rare events (e.g. nuclear security events) and more common events (e.g. floods or earthquakes). In this case, the likelihoods may vary by orders of magnitude.
(e) Custom weighting: In this approach, threat ratings are combined as in the average rating methodology, but the ratings for different attributes are weighted differently according to their perceived importance to the overall threat. (Recall that for averaging, all attributes are weighted equally.) For example, it may be considered more important for an adversary to have

sufficient technical capability to complete the attack successfully than for the adversary to have strong organizational capability. If that is the case, the technical capability estimate should have a stronger influence on the overall threat rating, and so the rating for technical capability should be given greater weight when calculating the 'average'.

5.15. An important benefit of providing threat ratings is that they may be transformed or interpreted as likelihood estimates, and such estimates can support quantitative risk assessment methodologies. An example of a defined threat scale is given in Table 3. These descriptions may also be applicable in a threat narrative approach. An example of a threat scoring process and word ladder is provided in Appendix II.

TABLE 3. EXAMPLE WORD LADDER DESCRIBING OVERALL THREAT LEVELS

Threat assessment rating	Description
Very high	Adversaries have an established capability and current intention to attack the target It is assessed that an attack is highly likely
High	Adversaries have the capability to attack the target and such an attack is within the group's current intentions It is assessed that an attack is likely
Medium	Adversaries have some capability to attack the target, and such an attack would be consistent with the group's intentions, or they have the capability, but their intention may depend on current circumstances It is assessed that an attack is possible
Low	Adversaries currently have little capability and/or intention to attack the target It is assessed that an attack is unlikely
Very low	Adversaries currently have no capability and/or intention to attack the target It is assessed that an attack is very unlikely

RISK ASSESSMENT METHODOLOGIES

5.16. In nuclear security, risk is generally considered to be a function of three components: threat, vulnerability and consequence. Risk assessment combines the estimated likelihood of particular nuclear security events, as an expression of the threat and vulnerability, with their consequences to provide an overall measure useful for the design or improvement of nuclear security systems and measures. A particular nuclear security event may be considered 'high risk' because it is considered likely to occur or because it would result in significant consequences, or both. By estimating expectation values of the economic loss due to possible nuclear security events, risk assessments can provide estimates that may, in some cases, be compared with the costs of systems and measures for preventing nuclear security events to evaluate the cost effectiveness of those systems and measures. In practice, such comparisons need to be made with great care to take due account of the uncertainty in the risk assessments and to avoid the impression that the evaluations are more reliable or accurate than they really are in order not to mislead the competent authorities responsible for implementation of the measures.

5.17. As with threat assessments, the level of detail and complexity and the extent of quantitative analysis in the risk assessment should be tailored to the prioritization decisions it is intended to support. Different risk assessment methodologies are appropriate for different domains of study. This subsection outlines two methods — one qualitative and one quantitative — that are commonly used and are considered appropriate for prioritizing the implementation of nuclear security systems and measures. These approaches are:

(a) Risk registry: A mapping of identified scenarios onto a matrix of likelihood and consequence scales for comparative visualization of risks. This methodology may be qualitative or semiquantitative.
(b) Probabilistic risk assessment: A scenario based approach that creates scenarios by combining principal elements or 'steps' leading to an event with consequences (usually shown graphically as an event tree, decision tree or fault tree) and estimating the ultimate consequences for each of the defined scenarios. This approach combines quantitative estimates of likelihood (or probability) for each principal element (called a 'node' in the event tree) to obtain overall likelihoods of scenarios. This methodology is similar to the probabilistic safety assessment [16].

5.18. Both of these approaches, but particularly the latter, depend upon the use of mathematical models to represent possible events and upon judgements by subject matter experts to define likelihoods (where these cannot be obtained from empirical observations of frequency) and other parameters [17]. The key principles for estimating risk using subject matter experts or models, and incorporating uncertainty in the estimates and results, are discussed in the following.

5.19. International industry standards on risk management identify three key steps in risk assessment: risk identification, risk analysis and risk evaluation [7]. Although the risk assessment methodologies described in this publication do not explicitly apply these names in the description of each step, they do include all three steps. Risk identification is addressed by scenario selection or scenario development in the methodology discussion. Risk analysis is addressed broadly through estimating likelihoods and completing risk calculations. Risk evaluation is addressed in the description of uncertainty analysis and sensitivity analysis.

Risk registry methodology

5.20. A risk registry is a list or catalogue of identified risks, similar to a risk register in project management. It documents the risk, the severity of the consequences and the likelihood of their occurring, and the actions to be taken to mitigate the risk. A worst case analysis is typically used for each generic risk, resulting in a small number of plausible representative scenarios. However, some techniques use a standard set of common (or nominal) scenarios with higher likelihoods. Such scenarios can serve as benchmarks for relative assessments within and across types of risk scenario. The severity of the consequences reflected in the risks often has several aspects and may include any or all of the following: human casualties, economic losses, societal disruption and environmental damage.

5.21. Risk registries are often used to compare disparate, broad types of risk (e.g. natural disasters, nuclear security events and industrial accidents) and to assist in allocating budgets across all hazards. Risk registries are often performed at a high level (i.e. strategic level), where estimates of relative likelihood and severity are elicited from subject matter experts, using logarithmic scales.

5.22. A risk registry should include the following components:

(a) Time frame: As the registry is a document that is regularly updated, it is important to record when the risks were estimated and the period for which the estimates are valid. Changes in risk may occur if there is a change in threat or a change in measures implemented to mitigate the risks. These changes should be incorporated in future assessments, as appropriate.

(b) Description of the risk: Since risk registries use small numbers of representative scenarios, the risk description should include all of the parameters that define each identified scenario and were used to evaluate the risk. Among these are:
   — The assumptions about the target;
   — The type of device;
   — The amount of material used;
   — The capability of the adversary;
   — Any assumptions reflecting judgements about the likely quality of the device (e.g. its reliability, efficiency or yield);
   — The assumed sequence of events that led to the nuclear security event;
   — Relevant conditions at the time of the event (e.g. weather or population affected);
   — The likely effectiveness of mitigation measures.

(c) Likelihood or frequency of occurrence: This is an assessment of how likely it is that the event will occur (expressed as probabilities or odds, e.g. low (<30%), medium (31–70%) or high (>70%) probability) or how frequently it might be expected to occur (expressed as frequencies, e.g. 10 times a year, once a year, once in 10 years, once in 100 years). Likelihoods of events may be evaluated on an absolute scale if desired, but it is usually more important (and often more reliable) to evaluate events in terms of relative frequency or likelihood (e.g. nuclear terrorism is much less likely than a flood and much more likely than an asteroid destroying the Earth). Depending on the objective, a relative scale may be sufficient to evaluate the risks.

(d) Severity of effect: This is an assessment of the possible consequences of a nuclear security event. This may include several separate assessments of different consequences, and these may be combined into a single overall assessment. As with likelihoods, relative measures of severity may be more important (and more usable) than absolute estimates of consequences.

(e) Additional countermeasures: These are actions to be taken to prevent or reduce the consequences of the event. They may include the planned response actions, which may already be taken into account in the likelihood and severity calculations. They may also include possible specific actions

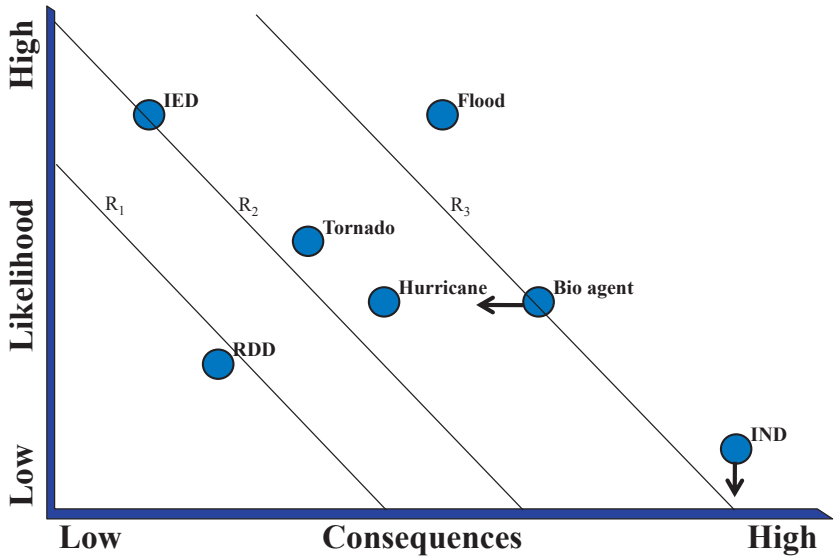
that could be taken to reduce either the likelihood or severity of particular events. In the latter case, the use of the countermeasures is often displayed as an arrow on the risk registry chart, showing the size and direction of risk reduction that the countermeasure could provide.

5.23. Figure 4 shows an example of a risk registry diagram with notional data. In this example, the diagram shows that the IND scenario has the greatest consequence but the lowest likelihood. Floods may be approximately as likely as the use of an improvised explosive device (IED) but with much greater consequences. The arrow on the symbol for biological agent attack ("Bio agent") indicates the potential reduction in consequences (but not likelihood) by using a particular medical countermeasure. The arrow from the IND symbol shows the reduction in likelihood (but not consequences) of an IND attack that could be achieved by implementing improved nuclear security measures. Other measures or combinations of measures might reduce both the likelihood and the consequences. In such cases, the arrows would point diagonally to the new likelihood and consequence associated with the reduced risk. Lastly, the diagonal lines are lines of equal risk: all points on the line have the same risk rating. Such lines can help decision makers in comparing different scenarios with the same level of risk.

Probabilistic risk assessment methodology

5.24. Probabilistic risk assessment can be used to assess the risk from various specified scenarios in a quantitative or semiquantitative fashion. When evaluating risks from nuclear security events, the scenarios are typically constructed from key elements, usually represented as a fault tree, event tree or decision tree.

5.25. A probabilistic risk assessment approach provides a systematic method for constructing risk scenarios by defining the important elements of a nuclear security event and constructing a 'scenario space' encompassing all possible instances of each of the elements. The important elements may be such things as an adversary's decisions on a particular course of action from among various options, the success or failure of intermediate steps in the adversary's course of action, or the effectiveness (or otherwise) of nuclear security measures in impeding the adversary's actions. These elements may be described and presented as branching points in an event tree, where different paths through the tree represent different individual scenarios. Each branching point is called a node, or a level, in the tree. The end nodes of the tree (from which no additional branching occurs), sometimes called leaves, represent different ultimate outcomes. To calculate risk, consequences are estimated for each of the

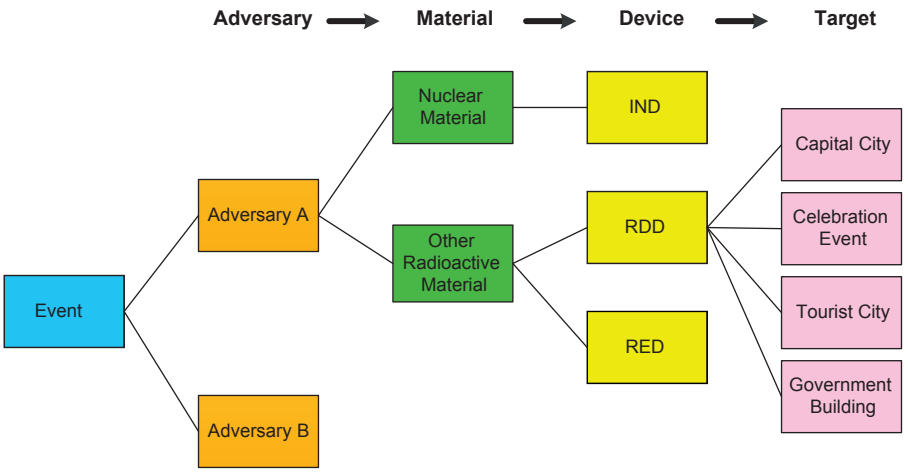


Note: All likelihood and consequence estimates are notional and do not reflect real values. R1 < R2 < R3 (lines represent equal risk). IED — improvised explosive device; IND — improvised nuclear device; RDD — radiological dispersal device.

FIG. 4. Example all hazards risk registry used for prioritizing resources among all hazards.

end nodes of the tree separately. The competent authority should decide which consequences it considers relevant (e.g. casualties, environmental contamination, economic impacts and societal impacts) and should therefore be estimated. The likelihood of any scenario is calculated as the product of the likelihoods for each of the branches that make that scenario from the tree.

5.26. The tree is constructed by identifying the different possibilities for each node in the tree. Part of a simple example event tree is shown in Fig. 5. In the example, two adversary groups are considered, along with two types of material that they might acquire and with which they might construct several types of device. Four possible targets are considered in this example. In practice, the number of possible targets may be much larger than this, or targets may be described as broader categories or types of target, rather than particular buildings or events.



Note: Only part of the tree is shown. IND — improvised nuclear device; RDD — radiological dispersal device; RED — radiation exposure device.

FIG. 5. Example event tree for developing risk scenarios.

5.27. The next step is to evaluate the likelihood of each path through the tree. In this example, combining all possibilities for all of the pathway nodes would generate 48 individual scenarios, and the competent authority needs to estimate the likelihood of each choice at each node in order to allow the likelihood for each of the scenarios to be calculated.

5.28. The tree shown is intentionally very simple for illustration purposes and does not address all of the issues involved in performing a probabilistic risk assessment. In practice, the estimation of likelihoods may depend on other nodes, and additional modelling or calculation may be needed to obtain values for likelihoods at nodes where the possibilities are complex. The tree provides an example of how a complete set of scenarios may be constructed using an event tree. A carefully constructed tree should allow the identification of a full range of plausible scenarios and give confidence that the results capture all of the significant risks from potential nuclear security events.

Assessing likelihood of risk scenarios

5.29. A key factor in understanding risk is estimating the likelihood of different types of potential nuclear security event, which is an inherently uncertain process. This subsection describes general approaches to assessing likelihood, their

respective advantages and disadvantages, and the resources needed to conduct the analysis. A comparison between absolute estimates and relative estimates is also presented. The main considerations are as follows:

(a) Likelihoods are often quantified so that they can be used in risk assessment where risk depends on the probability that a criminal or intentional unauthorized act involving nuclear material or other radioactive material is attempted and on the probability that the attempt is successful (as well as consequences).
(b) The estimation of likelihood is inherently uncertain, and therefore it is important to estimate not just the likelihood but the uncertainty in the estimated likelihood. This can be described as an error in the estimate (i.e. ± an absolute or proportionate amount), a probability distribution or by using words to imply approximate numbers.
(c) Likelihood may be estimated as an absolute probability or frequency. However, this approach is often very difficult and may not be necessary when applying risk assessment in evaluating alternatives. Relative likelihood (i.e. which of a set of scenarios is more likely and by how much) may be more easily estimated and may be sufficient unless the likelihood of these attacks must be compared with other hazards.

5.30. One approach to estimating likelihoods is to elicit probability values from subject matter experts. This approach allows the risk assessment to benefit from the expertise and knowledge within the State and to be specific to national circumstances and to specific scenarios. However, expert elicitation can be a very time consuming process, and may be sensitive to numerous structural biases if not conducted with great care. Techniques to avoid or mitigate the effects of these biases can be found in IAEA Safety Standards Series No. RS-G-1.9, Categorization of Radioactive Sources [18].

5.31. Alternatively, models may be developed to generate probability estimates. Models may span a wide range of possible scenarios and may be more flexible and suitable for analysis of larger numbers of alternatives. Some examples of types of modelling often used for such purposes are event trees, fault trees and game theory models. A comprehensive review of modelling approaches can be found in Ref. [19].

Uncertainty analysis

5.32. All risk assessments deal with uncertain data and judgements, limitations on the ability to predict or model real events, and uncertain or ambiguous results.

Each of these aspects of dealing with uncertainty should be addressed through techniques such as the following:

(a) The uncertainties in inputs to a risk assessment derived from experts should be identified as part of the elicitation or modelling process. Uncertainty is usually described by a distribution of possible values. Subject matter experts may be asked to provide estimates of multiple points of the distribution (e.g. the mean and extremes on each side of the mean, often the 5th and 95th percentiles), and these may be interpreted taking account of an understanding of how the distributions may be skewed or biased. In the case of modelling, statistical methods may be used to derive distributions of the estimates of inputs to risk assessment.
(b) The uncertainty in inputs should be taken into account throughout the risk calculations, along with other uncertainties associated with those calculations. Since it rapidly becomes mathematically intractable to calculate distributions directly for multiple uncertainties in multiple parameters, other techniques, such as Monte Carlo sampling, are often used to estimate the uncertainty distributions in the results [20].
(c) It is essential to convey to decision makers the uncertainties in the inputs to, and calculations within, the risk assessment and consequently in the results. When results are presented numerically (e.g. risks), the estimates should include an indication of the range rather than only a single number, and misleading indications of precision (e.g. quoting uncertain results to several significant figures) should be avoided in reporting results.

5.33. Uncertainty analysis is important because it provides a defensible indication of the reliability of risk assessment results as a basis for making decisions. Especially when issues are complicated or controversial, having validated and verified models that incorporate uncertainty helps to ensure that decisions can be based on the best available information.

6. USE OF RISK INFORMED APPROACHES

6.1. The potential consequences of a nuclear security event could be catastrophic. States should therefore take all appropriate steps to prevent them. However, States do not have unlimited resources, and therefore a State should have methods to identify which nuclear security measures are likely to be

most effective in reducing the risk. A risk informed approach can be used to assist States in evaluating options and prioritizing nuclear security measures.

6.2. A risk informed approach is an iterative process that: identifies and assesses risks; develops, evaluates, selects and implements measures to reduce the risks; monitors the effectiveness of the resulting measures; and makes adjustments as necessary [7]. A risk informed approach can be used to guide sound prevention, detection, response, mitigation and recovery efforts to minimize risks. It supports a wide variety of decisions including: strategic planning; policy making; budget setting; prioritizing research and development; and designing operational activities for nuclear security.

6.3. An iterative risk informed approach should aim to continually improve and enhance the nuclear security systems and measures of a State over time. An example of such an approach is illustrated in Fig. 6. The five main steps in this example are described in the following paragraphs.

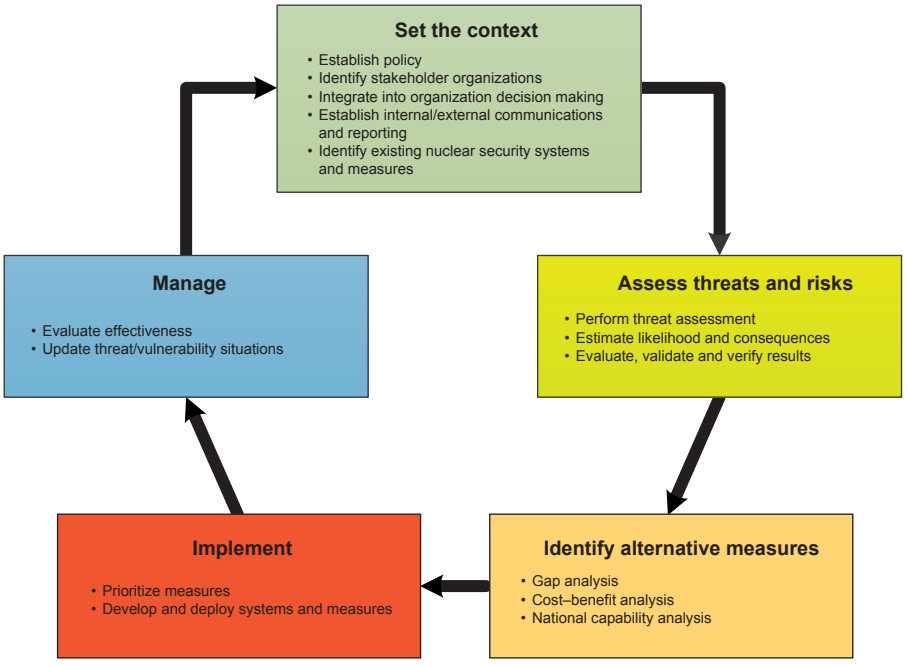


FIG. 6. Example of a risk informed approach for implementation of nuclear security systems and measures.

6.4. The cycle is repeated on a periodic basis (timed to support a need for decisions or a significant change in circumstances) to improve the analysis and results, and the effectiveness of the nuclear security systems and measures. Communication and consultation among internal and external stakeholders is important throughout the process to ensure that the State's objectives are achieved.

6.5. The threat assessment, as well as being incorporated into the risk assessment portion of the risk informed approach, also has an integral role in the identification of risks. It is also important in the evaluation of alternative strategies or systems and measures for nuclear security (since an adversary may be expected to adapt to changes in such measures), and in the monitoring of trends in threats' behaviour and in the effectiveness of the nuclear security systems and measures.

SETTING THE CONTEXT

6.6. In this step, the designated competent authorities identify which types of risk will be managed, who is responsible for managing them, which decisions depend upon risk information (and which type of information) and who the stakeholders are for the application of the risk informed approach. In addition, resources are identified for implementing the risk informed approach, including the necessary budget, people and organizational structure. Communication processes among stakeholders are developed, and an initial survey of nuclear security functions and activities are performed.

ASSESSMENT OF THREATS AND RISKS

6.7. In this step, the designated competent authority assesses the risks with the current nuclear security policies, systems and measures. As part of this step, the designated competent authority estimates the threat, vulnerability and consequences of possible nuclear security related actions by various adversaries. The assessment methodology should be tailored to the type of decision being made, the amount and quality of data available, and the level and type of resources available. Methods may range from a simple tabletop exercise with subject matter experts to detailed risk calculations. Regardless of the method chosen, it is important to maintain transparency in the methodology used so that decision makers can feel confident in the validity of the process and data.

IDENTIFICATION OF ALTERNATIVE NUCLEAR SECURITY SYSTEMS AND MEASURES

6.8. Using the outcomes of the risk assessment, competent authorities responsible for the implementation of nuclear security systems and measures should be able to identify potential improvements to better address high priority risks of criminal or intentional unauthorized acts involving nuclear and other radioactive material out of regulatory control. Examples of alternative nuclear security measures could include additional security or strengthened protection capabilities for regulated facilities and activities, enhanced border monitoring capabilities or law enforcement awareness, or new protocols and procedures to protect particular targets. The concept of defence in depth should be considered in the identification, prioritization, and design of nuclear security systems and measures.

6.9. The designated competent authorities may apply the following three common approaches to identifying and evaluating alternatives: gap analysis, cost–benefit analysis and national capability analysis.

Gap analysis

6.10. A gap is present when there is no adequate capability to address a viable threat. Gap analysis involves finding elements or functions of the nuclear security systems and measures, considered necessary in the light of the threat assessment, that do not exist, are not performed or do not address the relevant threats. Gaps are often identified by examining the threats that lead to the highest risks and identifying opportunities to defeat those threats by adding capability, changing operations or reducing vulnerabilities.

Cost–benefit analysis

6.11. Cost–benefit analysis compares the cost of a nuclear security measure with the benefit it provides (risk reduction). The analysis should consider the full life cycle costs of the measure, which may include equipment, installation, operation, maintenance, human resources and training costs, as well as upgrades or decommissioning costs. The risk reduction is usually converted into monetary terms to allow comparison with the costs of the measure. This supports a graded approach to improving nuclear security systems and measures. Some ‘costs’ of the measures may also be of a non-monetary nature, such as changes to plans and procedures, and the reallocation of assets.

National capability analysis

6.12. National capability analysis involves evaluating the entire set of nuclear security systems and measures as an integrated system to address the threat. This approach is often used when it is necessary to model the intentions of flexible adversaries, which may change depending on the particular nuclear security measures that are implemented. For example, increasing security at one strategic location may make an adversary more likely to attack a different location. Increasing security at both locations may make an adversary decide to try a different type of attack. Thus, the real value of increasing security at one location can only be evaluated in the context of how security is changed (or not) at other locations. The simplest approach to national capability analysis is to evaluate risk for several alternative complete sets of systems and measures, and to infer the value of a particular type of measure from how often it is included in the best performing sets.

6.13. When evaluating the risk effect of systems and measures, it is important to remember that adversaries may modify their approaches to respond to new or additional nuclear security measures. Typically, therefore, the overall risk reduction is less, as adversaries simply change tactics, compared with a situation in which the threat is static (i.e. the adversary only considers one type of attack on one target). Sometimes, increasing security in one place may encourage adversaries to change to another scenario that would have been more successful even under the previous systems and measures. In such a case, there could actually be an increase in overall risk from improving security in some places. Understanding adversaries' tendencies and likely responses can help ensure that additional security provides the intended risk reduction.

6.14. Since the responsibility for all the nuclear security systems and measures in a State is often divided among a number of different competent authorities, it is essential to coordinate the application of resources and the approaches to reducing risk. Proper coordination can help to ensure that systems and measures beneficial to the effective performance of one competent authority's responsibilities are deployed in a timely fashion by another competent authority.

IMPLEMENTATION OF NUCLEAR SECURITY SYSTEMS AND MEASURES

6.15. Once a State decides upon a course of action, the nuclear security systems and measures can be implemented (designed, deployed and maintained). Implementation should follow appropriate management practices to ensure that projects are completed to specification, on time and within budget.

6.16. After the nuclear security systems and measures have been prioritized and designed, implementation typically includes development, acquisition, deployment, operation, maintenance and sustainability of capabilities [11]. The protection of sensitive information and sensitive information assets related to the nuclear security systems and measures should be taken into account in the implementation.

6.17. A risk informed approach to prioritization and implementation is different from a risk based approach, in which risk is the primary and deciding factor in prioritization. There are many factors that should be considered in prioritizing nuclear security systems and measures (e.g. budgetary factors, political factors, feasibility and acceptability of the measures, performance or other costs induced by the measures). Risk is one factor that informs the overall prioritization decision and should be considered by decision makers in conjunction with these other factors.

MANAGEMENT OF RISKS

6.18. Deploying and implementing nuclear security systems and measures should not be a one-time action. The systems and measures should be operated, maintained and sustained, and should be upgraded or adapted as the situation changes. Systems and measures should be tested to ensure that they perform as designed. In this step, the effectiveness of the nuclear security systems and measures in practice should be re-evaluated (i.e. do they in fact work as well as intended). In addition, the threats and vulnerabilities should be continuously monitored to identify changes that affect the threat, such as information of new adversaries, changes in adversaries' objectives or capabilities, development of new nuclear security systems and measures and other factors. The results of the monitoring process should be used to update the context and risk analysis information for the next iteration of the risk informed approach cycle.

Evaluation of effectiveness

6.19. Effectiveness metrics are designed to measure how well the nuclear security systems and measures prevent, detect and respond to threats involving nuclear and other radioactive material out of regulatory control. In practice, calculating useful metrics is extremely difficult, since attempts to steal material or commit acts with nuclear security implications are extremely rare. In the absence of actual experience from real events, models or proxy measures should be developed.

6.20. Training exercises, taking into consideration all of the resources necessary for the functioning of nuclear security systems and measures, can indicate the performance of the measures and provide information about the overall effectiveness of the system as implemented. Typically, a combination of results from exercises, other performance measures (such as mean time between failures) and models could be used to estimate the performance of the nuclear security systems and measures.

Trend analysis

6.21. In addition to estimating the effectiveness of the nuclear security systems and measures against previously identified threats, it is important to update the assessment of threats to reflect changes in capabilities. For the trend analysis, considerations could include:

— Have known adversaries changed their behaviour? Have they demonstrated additional capabilities or expertise? Do they have new contacts with other non-State actors?
— Are there new adversaries that may consider acts with nuclear security implications?
— Have adversaries shown additional interest in the State as a target, a safe haven or a source for nuclear material or other radioactive material?
— Has commercial traffic or smuggling traffic changed appreciably through the State? Does greater volume require additional scrutiny?
— Have there been major modifications to the nuclear security systems and measures? Are there new locations being used for storage or use of nuclear material or other radioactive material, or have the amounts or types of such material available changed significantly?

6.22. Identifying the trends in threats and changes in the State's nuclear security systems and measures is an important step in determining when to update or initiate an iteration of the risk informed approach cycle. The cycle should be repeated periodically, in concert with decision processes. In addition, when there are significant changes to the State's nuclear security detection and response systems and measures [10, 11] or to the threat, the risk assessment should be reviewed and updated and the risk informed approach cycle repeated.

Appendix I

THREAT ASSESSMENT AND RISK INFORMED APPROACH TEMPLATE

I.1. The flowchart in this appendix (see Fig. 7) shows the complete risk informed approach cycle. All of the important steps described in this publication are incorporated into a single overall process.

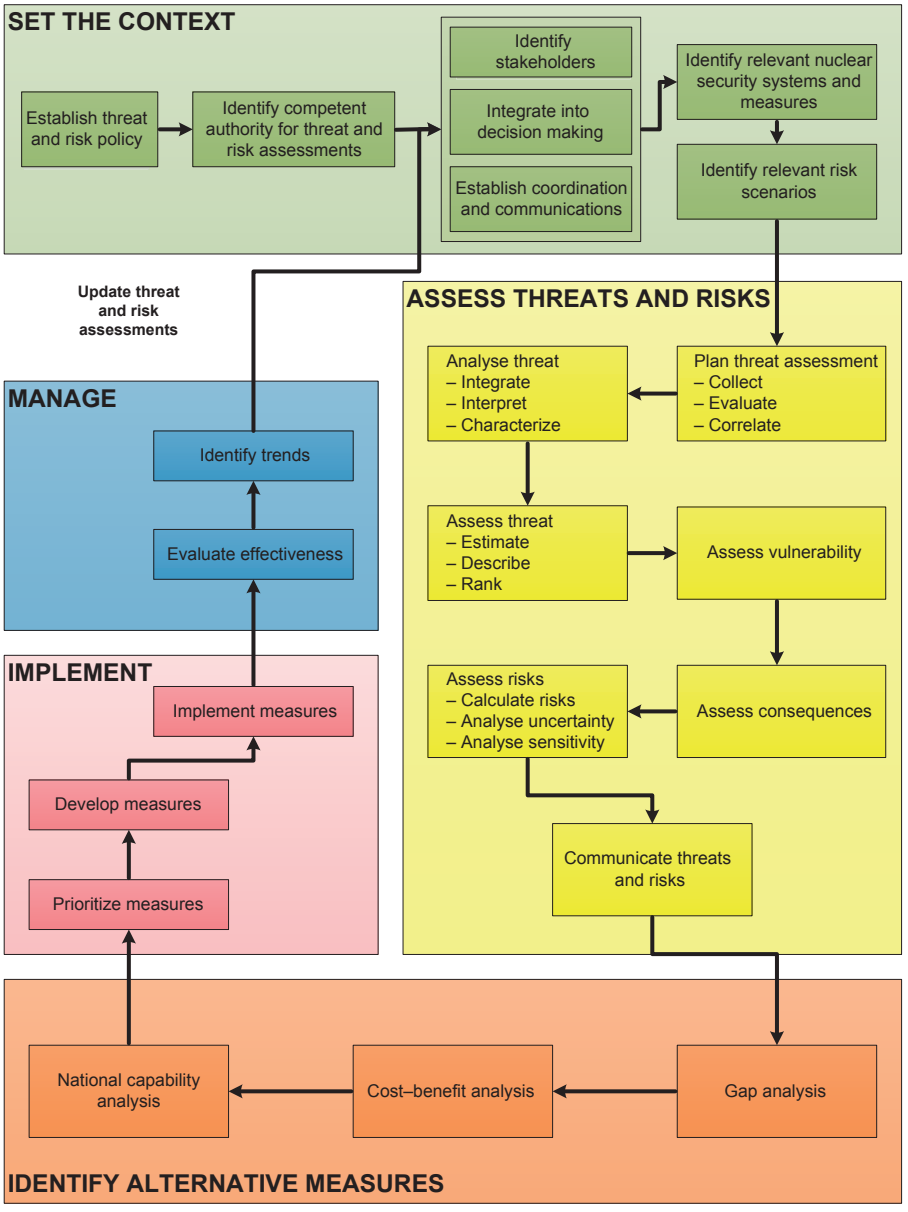


FIG. 7. Threat assessment and risk informed approach template.

Appendix II

THREAT ASSESSMENT EXAMPLE

ASSESSMENT CONTEXT

II.1. In the interests of brevity, all the reasoning, processes and analysis that underlie the assessments are omitted from this example. What is shown are example outputs of the processes and how results may be presented to stakeholders.

II.2. Throughout Appendices II–IV, a common, notional Example State is assumed. The Example State has a nuclear power plant and a research reactor, but not a full nuclear fuel cycle. The Example State also has hospitals that store and use radioactive material and sources and other industries (e.g. construction) that have significant number of radioactive sources that are licensed through the Example State regulatory authority.

II.3. The responsibility for regulating nuclear material and other radioactive material within the associated facilities and associated activities as well as detecting and responding to nuclear security events lies with several Example State competent authorities. All of these authorities cooperate and work collaboratively with the competent authority responsible for threat and risk assessments to implement a risk informed approach for nuclear security measures involving nuclear and other radioactive material out of regulatory control. Furthermore, the competent authority of the Example State outlines the known gaps, relevance and timeliness of information and intelligence used in support of the threat assessment.

II.4. There are several decision processes that could benefit from a risk informed approach that would help to prioritize scarce resources. There is optimism within the Example State that a risk management process will help to conserve resources.

IDENTIFICATION OF MATERIAL AND ADVERSARIES

II.5. The competent authority of the Example State conducts a threat identification process that considers adversaries and nuclear and other radioactive material out of regulatory control. Incident analysis of ITDB data shows that:

(a) Construction gauges containing radioactive material have been stolen and not recovered within the Example State.
(b) There are more than three times as many incidents recorded in the neighbouring State to the west as in the States to the north, east and south.
(c) Nuclear material suitable for an IND has never been lost, missing or stolen in the State or in neighbouring States; however, the potential for acquisition from these States or another State cannot be completely discounted.

II.6. The competent authority assesses and decides that there are three classes of potential adversaries to consider in determining the threat and risk:

(a) An international adversary group that may either carry out an act within the Example State's borders or use the Example State as a staging ground for committing an act against another State.
(b) A domestic adversary group that has advocated the overthrow of the current government and has carried out other violent acts.
(c) An individual or small group with a specific agenda and a tendency towards violence.

II.7. The competent authority provides the threat analysts with information about group tendencies and known plans and objectives. Recent related incidents (either acts that indicate group tendencies or acts that are related to nuclear security) are collected and correlated.

IDENTIFICATION OF TARGETS

II.8. The Example State competent authority for threat and risk assessments identifies several key potential targets for acts involving nuclear or other radioactive material out of regulatory control. These are viewed as the primary targets for the threat analysis:

— The downtown area of the Example State's capital city;
— The main shopping district of the Example State's primary tourist city;

— Several critical government buildings housing key agencies of the Example State;
— The annual national day celebration.

II.9. Since the Example State has a relatively small number of identified targets, these targets are assessed individually. If the competent authority decided to assess many more potential targets, the targets could be grouped into target types.

IDENTIFICATION OF CONSEQUENCES

II.10. The Example State competent authority convenes a group of experts on explosives, radiation and criminal or intentional unauthorized acts to evaluate the likely consequences of a set of potential acts against the identified targets. The experts consider many variables that can influence the actual consequence values including the amount and type of radioactive material, the meteorological conditions at the time of the act, the nature of the target and the characteristics of the act itself. The group then provides order of magnitude estimates of the consequences for a set of scenarios. The estimates can be provided for casualties and economic costs for each scenario (for simplicity, the economic costs include environmental and societal consequences). The combined consequence value (Value) and the normalized consequence rating can be calculated as follows:

$$\text{Value} = \text{Casualties} \times \text{Nominal casualty value} + \text{Economic} + \text{Environmental} + \text{Societal} \quad (1)$$

$$\text{Normalized consequence rating} = 100 \times \frac{\text{Value}}{\text{Max (Value)}} \quad (2)$$

II.11. Since the goal of the competent authority is to assign a relative severity to the scenarios, the casualties can be multiplied by an average cost value of one million currency units (for illustration purposes) and added to the economic costs to make a combined cost measure. The resulting values can be normalized by the highest value to create a normalized consequence rating from 0 to 100. The consequence table that results from this analysis is shown in Table 4.

TABLE 4. RELATIVE SEVERITY OF NOTIONAL SCENARIOS FROM EXAMPLE STATE

Scenario	Human health (No. of casualties)	Economic cost (millions of currency units)	Normalized consequence rating
IND at a capital city	20 000	250 000	100
IND at a tourist city	10 000	100 000	40.74
RDD at a capital city	500	500	0.37
RDD at a government building	20	100	0.04
RDD at a celebration	2 000	250	0.83
RED at a tourist city	150	10	0.06
RED at a celebration	350	50	0.15
RED at a government building	15	5	0.01
Contamination event	800	250	0.39

Note: Numbers are hypothetical and are not intended for use outside the example. IND — improvised nuclear device; RDD — radiological dispersal device; RED — radiation exposure device.

THREAT ASSESSMENT

II.12. The Example State competent authority for threat and risk assessments coordinates efforts by various competent authorities to derive a threat narrative for the three adversary types identified. The experts are provided with data and charts showing known or suspected incidents of illicit trafficking in nuclear material or other radioactive material. The incidents are then broken down by type of material, location and incident, and the origin or legitimate use of the material. Reports describing the stated goals, recent activities and rhetoric from each of the known groups are also provided to the subject matter experts to enable a common assessment and approach from the group. Table 5 documents an example of such a consensus derived by the experts.

TABLE 5. EXAMPLE THREAT NARRATIVE ANALYSIS CHART FOR THREE ADVERSARIES

Adversary	Intent	Capability
International group	The group seeks to inflict high economic costs or mass casualties.	The group has sought to purchase or steal radioactive material, but their plots have been disrupted by law enforcement. The group has obtained extensive funds through criminal activities, but internal security measures have made it difficult for them to recruit technical experts or connect with individuals with access to radioactive material.
Domestic group	The group's goal is to inflict economic costs on the Example State government in order to achieve territorial autonomy, without mass casualties that would result in international outrage.	The group has a clear hierarchy based on family ties and engages in profitable crimes such as drug trafficking. None of the known members has an advanced university degree in physics or engineering, although they have demonstrated the ability to construct improvised conventional weapons. They have never attempted to purchase nuclear material or other radioactive material in the past.
Single adversary	The single adversary primarily aims to inflict a cost on the employer and embarrassing them. While the individual may be satisfied with serious injury or death, causing mass casualties is not part of the goal.	The individual has access to nuclear material or other radioactive material and the expertise to handle it, but has never constructed a complete device. Thus, only actions involving a radiation exposure device or causing limited contamination are likely to be taken.

II.13. Using a threat ranking approach, the competent authority responsible for threat and risk assessments also conducts a subject matter expert elicitation to rate each of the specific scenarios in conjunction with the adversary types. The specific approach divides the assessment into several subcategories. Capability can be divided into organizational, technical and financial. Intent can be divided into ideology and objective. The likelihood of creating a device can be divided into the material, the difficulty of acquiring the material and the difficulty of constructing the device. Lastly, the vulnerability of the target can be divided

into the type of target and the timing of an attack. Each of these criteria or factors is assessed based on defined rating scales (also referred to as 'word ladders') that establish the criteria of each rating level. An example for the assessment of a certain domestic insurgent group deploying an RDD at an annual celebration is shown in Tables 6–8 and described in paras II.14–II.16.

TABLE 6. EXAMPLE CAPABILITY AND INTENT THREAT RANKING

Threat assessment component ratings	Capability			Intent	
	Organization	Technical expertise	Financial/ logistical	Ideology/ tendencies	Objective/ motive
Very high					
High					
Medium					
Low					
Very low					

TABLE 7. EXAMPLE MATERIAL AND VULNERABILITY THREAT RANKING

Threat assessment component ratings	Material			Vulnerability at target	
	Material type	Acquisition	Device	Target type	Opportunity/ time frame
Very high					
High					
Medium					
Low					
Very low					

TABLE 8. EXAMPLE SUMMARY THREAT RATING

Threat assessment overall rating
Very high
High
Medium
Low
Very low

II.14. The domestic group has a strong organization and is well funded but has not demonstrated an interest in or knowledge of nuclear material or other radioactive material. While they do not typically seek to cause civilian casualties, they are strongly motivated to carry out an act that increases their profile and credibility.

II.15. The desired radioactive material is available in the Example State, but access to it is tightly controlled. Once material is acquired, however, a device is easy to construct. The target is civilian and highly vulnerable, but timing is very limited to ensure maximum impact.

II.16. Overall, the combination of factors results in a high threat rating for the domestic group deploying an RDD at the Example State's annual celebration: the capability and intent are both rated high; and the attractiveness of material and target are rated high to very high. How this assessment is conducted — and the overall threat rating — will depend on the methodology used.

II.17. Similar assessments performed for each adversary–scenario pair are used to rate the potential acts. These rankings support relative likelihood estimates for the assessed options of nuclear security events using nuclear and other radioactive material out of regulatory control. This overall assessment would be substantiated based on the supporting evidence for each criterion assessment and validated through subject matter expert review.

Appendix III

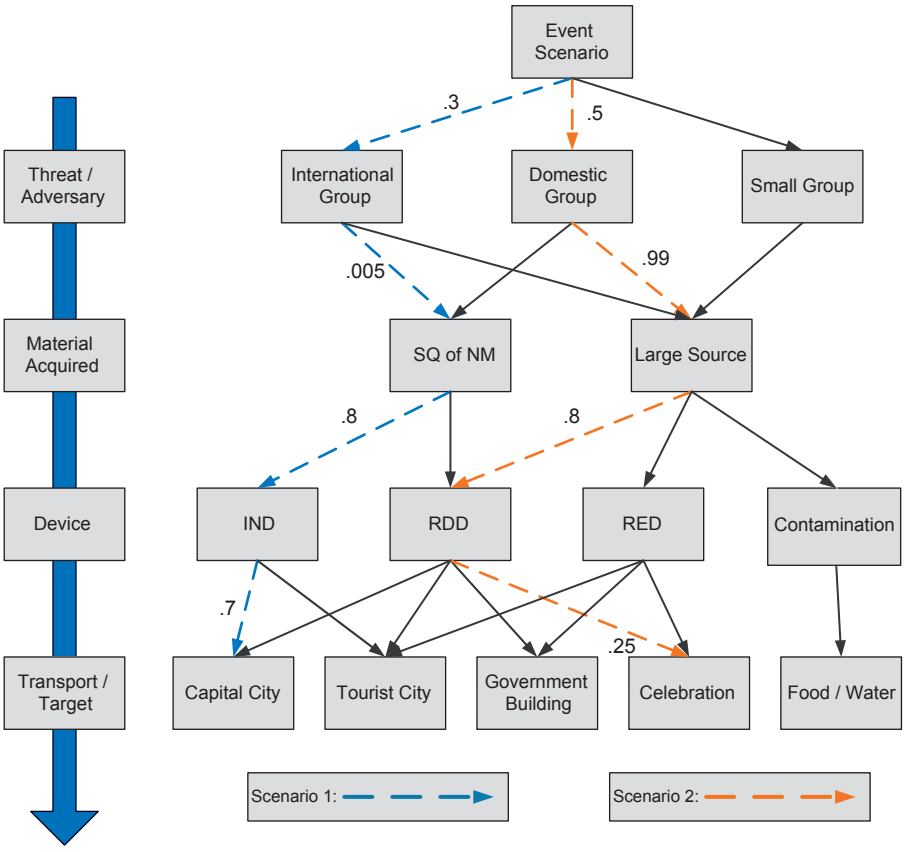
RISK ASSESSMENT EXAMPLE

III.1. The following example demonstrates the use of probabilistic risk assessment methodology by creating an event tree for the Example State. The values that make up the likelihood calculations for the tree's scenarios are estimated and sample analysis results are presented. This example builds upon the threat assessment example in Appendix II and uses its results.

SCENARIO STRUCTURE

III.2. The tree nodes and all alternatives at each node are presented in Fig. 8. This tree represents a minimum set of the types of node needed to describe nuclear security events involving material out of regulatory control. For simplicity, the number of alternatives at each node is kept to a minimum. The likelihood of each of the nodes is treated as a probability distribution. As is typical in such an event tree, the likelihood at some nodes is dependent on the values at other nodes. For example, the device node is dependent on the material acquired. It may be necessary or desirable to introduce additional dependencies in a State's risk assessment efforts.

III.3. A particular scenario created by the event tree is represented by a path through the tree. For example, one scenario would be a domestic group obtaining a large source, deciding to use it as an RDD to attack the annual celebration (Scenario 2 in the figure, indicated in orange). The tree shown, when fully expanded, could contain up to 120 scenarios (three possible adversaries × two types of material × four types of device × five potential targets). However, when unrealistic combinations are removed (e.g. a large gamma source is not suitable for the construction of an IND, an IND may not be considered for the contamination of food and water), the total number of self-consistent scenarios remaining in the risk model is reduced to 36. The risk assessment is completed by estimating the likelihood of each of the scenarios and estimating the consequences if the scenario occurs. The consequences were previously estimated in Appendix II, and relevant consequence estimates are listed in Table 4, in Appendix II. For the purposes of the risk assessment, the normalized consequence rating is used for the consequence estimates.



Note: In the example event tree, there are two types of material that may be acquired, a large source (Category 1 source [18]) and a significant quantity of nuclear material (SQ of NM). IND — improvised nuclear device; RDD — radiological dispersal device; RED — radiation exposure device.

FIG. 8. Event tree with two example scenarios highlighted.

LIKELIHOOD ESTIMATION

III.4. Estimating the likelihood of the scenarios is accomplished by estimating the likelihood of each of the scenario elements (accounting for dependencies where relevant). For the Example State, some example likelihood estimates are given in Fig. 8. The likelihood estimates provided in the figure are relative likelihoods for each level in the tree. In other words, for a given alternative in one level of the event tree, the likelihood value estimates the relative likelihoods of the alternatives in the next level down. Estimates such as these may be obtained from subject matter experts and in a full risk assessment should incorporate uncertainty

distributions. It is important to note that only the possible branches of the event tree are assigned likelihoods. In Fig. 8, 23 estimates are sufficient to determine likelihoods for all the scenarios.

RISK ASSESSMENT

III.5. Scenario risk is evaluated by calculating the scenario likelihood and multiplying by the consequence rating value (normalized consequence ratings are listed in Table 4, in Appendix II). For this example, a spreadsheet can be used to perform all the scenario expansion and calculation automatically. However, the example in Table 9 illustrates the calculation for the two highlighted scenarios in Fig. 8.

TABLE 9. EXAMPLE RISK CALCULATIONS FOR TWO SCENARIOS

Scenario 1: An international group obtains an SQ of NM and deploys an IND in the capital city		
Likelihood =	0.3 × 0.005 × 0.8 × 0.7	= 0.000 84
Scenario risk[a] =	0.000 84 × 100	= 0.084
Scenario 2: A domestic group obtains a large radioactive source and deploys an RDD at the celebration		
Likelihood =	0.5 × 0.99 × 0.8 × 0.25	= 0.099
Scenario risk =	0.099 × 0.83	= 0.082

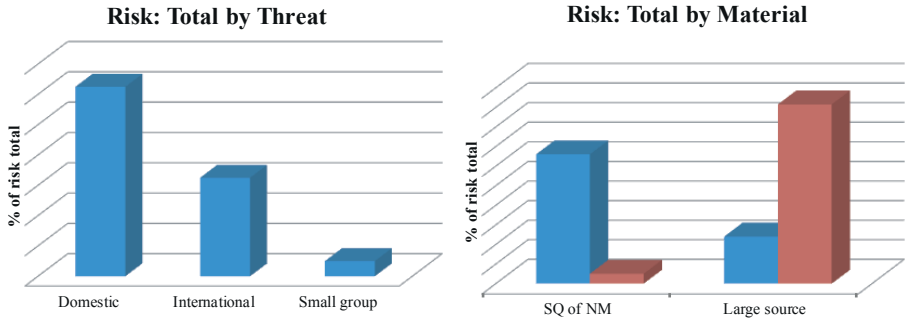
Note: IND — improvised nuclear device; RDD — radiological dispersal device; SQ of NM — significant quantity of nuclear material.

[a] Scenario risk = Likelihood × Normalized consequence rating. See Table 4, Appendix II.

III.6. Scenario 1 is an IND deployed in the capital city. Scenario 2 is an RDD deployed at the annual celebration. Scenario 2 is assessed to be approximately 100 times more likely than Scenario 1 (0.099 compared with 0.000 84), but Scenario 1 results in nearly 100 times greater consequences (100 compared with 0.83). The difference in relative likelihoods is balanced by the difference in consequences so that the two scenarios are of approximately equal risk. Thus, the risk values are used for comparison between scenarios and not as some absolute value of risk.

III.7. The descriptions of Scenarios 1 and 2 provide detailed information about the calculation of two specific scenarios. There are many more scenarios in the overall risk assessment, and it is often not possible to examine each scenario individually. Instead, scenarios are grouped by their characteristics (e.g. same adversary or same material). Useful depictions of the risk may be developed by taking a particular aspect of the risk (e.g. the adversary or the target) and examining the sum of risk over all scenarios associated with the particular threat group or target. For this example, two such depictions are shown in Fig. 9. It should be noted that in this example the individual scenarios for IND and RDD are of approximately equal risk, but when all the scenarios are considered the IND risk will be much greater than the RDD risk.

III.8. The figure on the left shows the risk from domestic, international and small adversary groups. In this case, the domestic group represents most of the risk and small groups the least risk. The figure on the right shows the difference between the risk and the likelihood of the two material types in the risk assessment. The blue bars in each pair represent the risk. In the diagram, SQ of NM represents the larger risk. The brown bars in each pair represent the likelihood of scenarios that use that material. The large source is by far the more likely. The difference between the risk and likelihood is accounted for by the consequences. Large sources could be used in other devices but INDs must contain nuclear material. However, INDs have the potential to cause much greater consequences (according to this notional example assessment) so that the difference in consequences outweighs the difference in likelihood. A significant portion of risk assessment involves understanding this interplay between likelihood, consequences and risk.



Note: The blue bars represent the risk. The brown bars represent the likelihood of scenarios that use that material. SQ of NM — significant quantity of nuclear material.

FIG. 9. Two examples of risk depiction.

III.9. Another key factor in understanding risk involves showing the uncertainty in the estimates. Figure 10 shows an example uncertainty chart of risk over potential target locations. In addition to the mean risk (represented by the bar for each target), the chart shows with a line the uncertainty in the risk estimate for each target. The top and bottom ends of the line for each target represent the 95th and 5th percentile of the uncertainty distribution, respectively, and are often calculated from uncertain probability distributions, using Monte Carlo techniques. On this chart, the analyst can identify the important distinctions in risk. For example, it is clear that the capital city is at greater risk than any other target; however, the tourist city and the annual celebration have overlapping uncertainty distributions.

III.10. Thus, it is vital in a risk assessment to understand how uncertainty affects the results. In some assessments with large uncertainties, it may be difficult to distinguish reliably between risks with higher and lower mean values. In many cases, only the outliers (highest and lowest risks) may be clearly discernible, with many risks of similar magnitude in between. Using only the mean values of risk tends to make the risk assessment seem more precise than is justified, and may therefore be misleading. These charts can assist a risk analyst in completing the risk assessment and communicating the risk to decision makers.

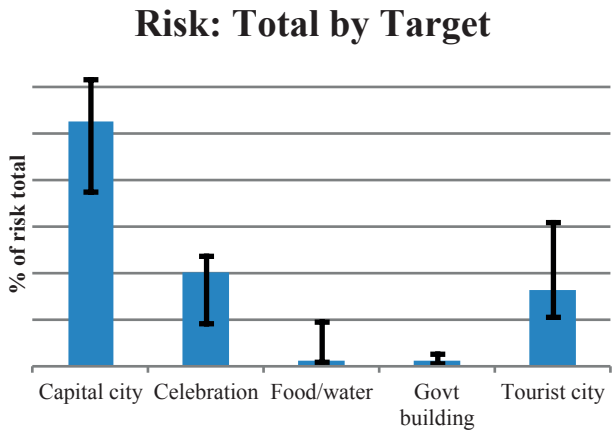


FIG. 10. Example risk plot including uncertainty bands.

Appendix IV

RISK INFORMED APPROACH EXAMPLE

IV.1. The following example demonstrates the use of the results of threat and risk assessments as part of a risk informed approach by using both their inputs and outputs (described in Appendices II and III, respectively). This appendix focuses on the latter half of the risk informed approach cycle: the analysis and choice of alternatives, the implementation of the selected systems and measures, and the ongoing management of the programme that includes updated threat assessments and evaluations of the effectiveness of implemented nuclear security systems and measures.

IDENTIFICATION, PRIORITIZATION AND IMPLEMENTATION

IV.2. Following the risk assessment described in Appendix III, the relevant competent authorities (the competent authority responsible for threat and risk assessments and the competent authorities responsible for security at the various targets) identify potential systems and measures that may be deployed to reduce the risk from an act with nuclear security implications. In some cases, only one measure may be evaluated; in other cases, multiple alternative measures may be evaluated. Table 10 lists the potential systems and measures to be evaluated. For each system or measure, the competent authorities estimate the reduction in the likelihood of the nuclear security event that the system or measure is expected to achieve, and the costs to implement the system or measure.

IV.3. These systems and measures are evaluated both individually and in combination to identify the amount of risk reduction for each level of expenditure. A graph of this cost–benefit analysis (where the benefit is defined as risk reduction) is shown in Fig. 11. Each point represents one security option (i.e. one possible set of systems and measures) at each of the target locations shown in Table 10. The boxes represent the set of selected options that may be implemented, one at a time, to optimally improve security. The security options providing the lowest risk per unit cost are on the blue line (labelled as “optimal security option”).

TABLE 10. POTENTIAL NUCLEAR SECURITY SYSTEMS AND MEASURES FOR THE EXAMPLE STATE

Target location	System or measure option	Description
Capital city	Baseline	Current existing capability in the capital city
	Added police	Increase number of police officers patrolling capital city
	Added sensors	Purchase and deploy radiation detectors around the capital city
Tourist city	Baseline	Current existing capability in the tourist city
	Enhanced procedures	Develop training and provide a support capability for tourist city police officers to recognize and identify nuclear security threats
Government building	Baseline	Current existing capability in government buildings
	Added physical protection	Improve physical barriers (locks, access systems, doors and windows, and concrete barriers) that protect buildings
	Security system	Install a security system with door and window alarms, some radiation detection, and video monitors
National day celebration	Baseline	Current existing capability to protect celebration
	Perimeter security	Improve perimeter security at celebration by setting up barriers and ensuring people enter the area through well defined bottlenecks where detection can occur
	Enhanced procedures	Develop awareness briefings and provide a reach back capability for police officers to recognize and identify nuclear security threats
	Increased patrols	Increase the number and reduce the predictability of patrols by security personnel during the celebration
Food and water	Baseline	Current existing capability at food processing plants and water systems
	Enhanced monitoring	Monitor specific food and water samples

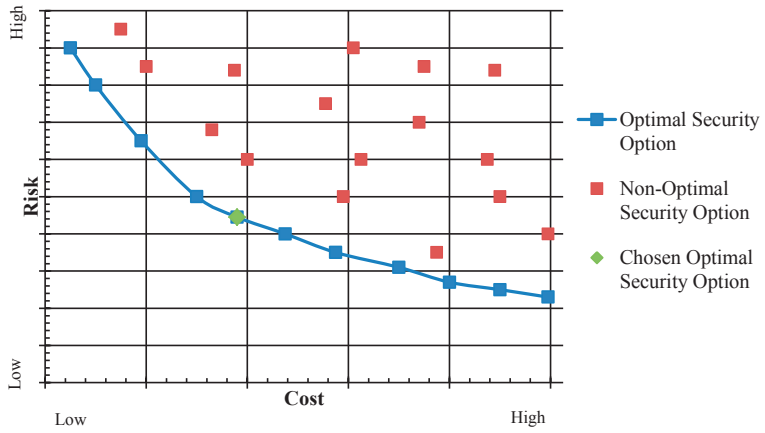


FIG. 11. Cost–benefit analysis chart showing security options and chosen option.

IV.4. Since the Example State can see that risk reduction tails off considerably after implementing the first four programmes, the competent authorities agree to implement the optimal selection at that point in the chart (marked as the chosen option). That option consists of the following improvements: adding police to the capital city, enhancing procedures in the tourist city, and setting up a security perimeter around the site of the annual celebration. It should be noted that other factors may affect the decision in addition to risk reduction. For this simple example, however, only the risk reduction is included in the selection.

MANAGEMENT OF RISKS

IV.5. The Example State implements the four sets of systems and measures in the chosen option, using best practice for programme management and system deployment. As part of the management approach, the capability of the perimeter for the annual celebration is exercised at a similar, but much smaller public event, and processes are modified to address issues and concerns arising from the exercise. The modified perimeter and processes are deployed at the annual celebration. The extra police for the capital city are hired and trained. While it is impossible to measure the potential performance of the new assets against potential acts with nuclear security implications directly (owing to their scarcity), reductions in crime are measured and used as a proxy for increased ability to prevent acts with nuclear security implications. In addition, a mock-up of a device is created and used as an unannounced exercise to test the awareness of the law enforcement authorities and to evaluate their ability to detect and

interdict a potential act. Lastly, the new procedures are developed for the tourist city and, following their implementation, the effects on tourists and local residents are assessed.

IV.6. The competent authority for threat and risk assessments maintains an awareness of potential material out of regulatory control by monitoring activity within the Example State as well as reports to ITDB and INTERPOL alerts. Periodically, the threat assessment is updated with new information about the different adversaries' intentions and capabilities. When the threat assessment is updated, the risk assessment is updated as well. The updated risk assessment is communicated within the Example State government via the competent authority on a need to know basis. In line with budgeting and procurement cycles, the complete risk management process is exercised as the Example State iteratively improves its ability to address acts with nuclear security implications arising from material out of regulatory control.

REFERENCES

[1] The Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev. 1, IAEA, Vienna (1980).

[2] International Convention for the Suppression of Acts of Nuclear Terrorism, Resolution A/RES/59/290, United Nations, New York (2005).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIR/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14, IAEA, Vienna (2011).

[6] EUROPEAN POLICE OFFICE, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL CRIMINAL POLICE ORGANIZATION–INTERPOL, UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE, UNITED NATIONS OFFICE ON DRUGS AND CRIMES, WORLD CUSTOMS ORGANIZATION, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 15, IAEA, Vienna (2011).

[7] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Risk Management: Principles and Guidelines, ISO 31000:2009, ISO, Geneva (2009).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Development, Use and Maintenance of the Design Basis Threat, IAEA Nuclear Security Series No. 10, IAEA, Vienna (2009).

[9] EUROPEAN POLICE OFFICE, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CRIMINAL POLICE ORGANIZATION, WORLD CUSTOMS ORGANIZATION, Combating Illicit Trafficking in Nuclear and other Radioactive Material, IAEA Nuclear Security Series No. 6, IAEA, Vienna (2007).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Systems and Measures for the Detection of Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 21, IAEA, Vienna (2013).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CRIMINAL POLICE ORGANIZATION–INTERPOL, UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE, Radiological Crime Scene Management, IAEA Nuclear Security Series No. 22-G, IAEA, Vienna (2014).

[13] STOIBER, C., CHERF, A., TONHAUSER, W., DE LOURDES VEZ CARMONA, M., Handbook on Nuclear Law: Implementing Legislation, IAEA, Vienna (2010).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Incident and Trafficking Database (ITDB): Incidents of nuclear and other radioactive material out of regulatory control, 2014 Fact Sheet (2014), http://www-ns.iaea.org/downloads/security/itdb-fact-sheet.pdf
[15] INTERNATIONAL CRIMINAL POLICE ORGANIZATION—INTERPOL, Guidelines on Criminal Intelligence Analysis, Version 4 (LEJEUNE, P., MASON-PONTING, J., Eds), Criminal Analysis Sub-Directorate, INTERPOL General Secretariat, Lyon (2002).
[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-3, IAEA, Vienna (2010).
[17] KEENEY, R.L., VON WINTERFELDT, D., Eliciting probabilities from experts in complex technical problems, IEEE Trans. Eng. Manage. **38** 3 (1991) 191–201.
[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Categorization of Radioactive Sources, IAEA Safety Standards Series No. RS-G-1.9, IAEA, Vienna (2005).
[19] LAW, A., Simulation Modeling and Analysis, 4th edn, McGraw-Hill, New York (2006).
[20] METROPOLIS, N., ULAM, S., The Monte Carlo Method, J. Am. Stat. Assoc. **44** 247 (1949) 335–341.

GLOSSARY

associated activity. The possession, production, processing, use, handling, storage, disposal or transport of nuclear material or other radioactive material.

associated facility. A facility (including associated buildings and equipment) in which nuclear material or other radioactive material is produced, processed, used, handled, stored or disposed of and for which an authorization is required.

authorization. The granting by a competent authority of written permission for operation of an associated facility or for carrying out an associated activity, or a document granting such permission.

competent authority. A governmental organization or institution that has been designated by a State to carry out one or more nuclear security functions. Competent authorities may include regulatory bodies, law enforcement, customs and border control, intelligence and security agencies, and health agencies.

graded approach. The application of nuclear security measures proportionate to the potential consequences of criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities, associated activities, or other acts determined by the State to have an adverse impact on nuclear security.

improvised nuclear device (IND). A device incorporating radioactive material designed to result in the formation of nuclear yield reaction. Such devices may be fabricated in a completely improvised manner or may be an improvised modification to a nuclear weapon.

nuclear material. Any material that is either special fissionable material or source material as defined in Article XX of the IAEA Statute.

nuclear security event. An event that has potential or actual implications for nuclear security that must be addressed.

nuclear security measures. Measures intended to prevent a nuclear security threat from completing criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities, or associated activities or to detect or respond to nuclear security events.

nuclear security system. An integrated set of nuclear security measures.

nuclear security threat. A person or group of persons with motivation, intention and capability to commit criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities or associated activities or other acts determined by the State to have an adverse impact on nuclear security.

other radioactive material. Any radioactive material that is not nuclear material.

out of regulatory control. See regulatory control.

radiation exposure device (RED). A device with radioactive material designed to intentionally expose members of the public to radiation.

radioactive material. Any material designated in national law, regulation or by a regulatory body as being subject to regulatory control because of its radioactivity. In the absence of such a designation by a State, radioactive material is any material for which protection is required by the current version of the International Basic Safety Standards.[1]

radiological dispersal device (RDD). A device to spread radioactive material using conventional explosives or other means.

---

[1] EUROPEAN COMMISSION, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, WORLD HEALTH ORGANIZATION, Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards, IAEA Safety Standards Series No. GSR Part 3, IAEA, Vienna (2014).

regulatory control. Any form of institutional control applied to nuclear material or other radioactive material, associated facilities, or associated activities by any competent authority as required by the legislative and regulatory provisions related to safety, security or safeguards. The term 'out of regulatory control' is used to describe a situation where nuclear or other radioactive material is present in sufficient quantity that it should be under regulatory control, but control is absent, either because controls have failed for some reason or they never existed.

risk. The potential for an unwanted outcome resulting from a nuclear security event as determined by its likelihood and the associated consequences.

risk assessment. The overall process of systematically identifying, estimating, analysing and evaluating risk for the purpose of informing priorities, developing or comparing courses of action, and informing decision making.

strategic location. A location of high security interest in the State which is a potential target for terrorist attacks using nuclear material or other radioactive material, or a location at which nuclear or other radioactive material out of regulatory control is located.

threat assessment. An evaluation of the threats — based on available intelligence, law enforcement and open source information — that describes the motivations, intentions and capabilities of these threats.

vulnerability. A physical feature or operational attribute that renders an entity, asset, system, network, facility, activity or geographic area open to exploitation or susceptible to a given threat.

vulnerability assessment. A process which evaluates and documents the features and effectiveness of the overall security system at a particular target.

IAEA
International Atomic Energy Agency

No. 23

ORDERING LOCALLY

In the following countries, IAEA priced publications may be purchased from the sources listed below or from major local booksellers.

Orders for unpriced publications should be made directly to the IAEA. The contact details are given at the end of this list.

AUSTRALIA
DA Information Services
648 Whitehorse Road, Mitcham, VIC 3132, AUSTRALIA
Telephone: +61 3 9210 7777 • Fax: +61 3 9210 7788
Email: books@dadirect.com.au • Web site: http://www.dadirect.com.au

BELGIUM
Jean de Lannoy
Avenue du Roi 202, 1190 Brussels, BELGIUM
Telephone: +32 2 5384 308 • Fax: +32 2 5380 841
Email: jean.de.lannoy@euronet.be • Web site: http://www.jean-de-lannoy.be

CANADA
Renouf Publishing Co. Ltd.
5369 Canotek Road, Ottawa, ON K1J 9J3, CANADA
Telephone: +1 613 745 2665 • Fax: +1 643 745 7660
Email: order@renoufbooks.com • Web site: http://www.renoufbooks.com

Bernan Associates
4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4391, USA
Telephone: +1 800 865 3457 • Fax: +1 800 865 3450
Email: orders@bernan.com • Web site: http://www.bernan.com

CZECH REPUBLIC
Suweco CZ, spol. S.r.o.
Klecakova 347, 180 21 Prague 9, CZECH REPUBLIC
Telephone: +420 242 459 202 • Fax: +420 242 459 203
Email: nakup@suweco.cz • Web site: http://www.suweco.cz

FINLAND
Akateeminen Kirjakauppa
PO Box 128 (Keskuskatu 1), 00101 Helsinki, FINLAND
Telephone: +358 9 121 41 • Fax: +358 9 121 4450
Email: akatilaus@akateeminen.com • Web site: http://www.akateeminen.com

FRANCE
Form-Edit
5 rue Janssen, PO Box 25, 75921 Paris CEDEX, FRANCE
Telephone: +33 1 42 01 49 49 • Fax: +33 1 42 01 90 90
Email: fabien.boucard@formedit.fr • Web site: http://www.formedit.fr

Lavoisier SAS
14 rue de Provigny, 94236 Cachan CEDEX, FRANCE
Telephone: +33 1 47 40 67 00 • Fax: +33 1 47 40 67 02
Email: livres@lavoisier.fr • Web site: http://www.lavoisier.fr

L'Appel du livre
99 rue de Charonne, 75011 Paris, FRANCE
Telephone: +33 1 43 07 50 80 • Fax: +33 1 43 07 50 80
Email: livres@appeldulivre.fr • Web site: http://www.appeldulivre.fr

GERMANY
Goethe Buchhandlung Teubig GmbH
Schweitzer Fachinformationen
Willstätterstrasse 15, 40549 Düsseldorf, GERMANY
Telephone: +49 (0) 211 49 8740 • Fax: +49 (0) 211 49 87428
Email: s.dehaan@schweitzer-online.de • Web site: http://www.goethebuch.de

HUNGARY
Librotrade Ltd., Book Import
PF 126, 1656 Budapest, HUNGARY
Telephone: +36 1 257 7777 • Fax: +36 1 257 7472
Email: books@librotrade.hu • Web site: http://www.librotrade.hu

INDIA

Allied Publishers

1st Floor, Dubash House, 15, J.N. Heredi Marg, Ballard Estate, Mumbai 400001, INDIA
Telephone: +91 22 2261 7926/27 • Fax: +91 22 2261 7928
Email: alliedpl@vsnl.com • Web site: http://www.alliedpublishers.com

Bookwell

3/79 Nirankari, Delhi 110009, INDIA
Telephone: +91 11 2760 1283/4536
Email: bkwell@nde.vsnl.net.in • Web site: http://www.bookwellindia.com

ITALY

Libreria Scientifica "AEIOU"

Via Vincenzo Maria Coronelli 6, 20146 Milan, ITALY
Telephone: +39 02 48 95 45 52 • Fax: +39 02 48 95 45 48
Email: info@libreriaaeiou.eu • Web site: http://www.libreriaaeiou.eu

JAPAN

Maruzen Co., Ltd.

1-9-18 Kaigan, Minato-ku, Tokyo 105-0022, JAPAN
Telephone: +81 3 6367 6047 • Fax: +81 3 6367 6160
Email: journal@maruzen.co.jp • Web site: http://maruzen.co.jp

NETHERLANDS

Martinus Nijhoff International

Koraalrood 50, Postbus 1853, 2700 CZ Zoetermeer, NETHERLANDS
Telephone: +31 793 684 400 • Fax: +31 793 615 698
Email: info@nijhoff.nl • Web site: http://www.nijhoff.nl

SLOVENIA

Cankarjeva Zalozba dd

Kopitarjeva 2, 1515 Ljubljana, SLOVENIA
Telephone: +386 1 432 31 44 • Fax: +386 1 230 14 35
Email: import.books@cankarjeva-z.si • Web site: http://www.mladinska.com/cankarjeva_zalozba

SPAIN

Diaz de Santos, S.A.

Librerias Bookshop • Departamento de pedidos
Calle Albasanz 2, esquina Hermanos Garcia Noblejas 21, 28037 Madrid, SPAIN
Telephone: +34 917 43 48 90 • Fax: +34 917 43 4023
Email: compras@diazdesantos.es • Web site: http://www.diazdesantos.es

UNITED KINGDOM

The Stationery Office Ltd. (TSO)

PO Box 29, Norwich, Norfolk, NR3 1PD, UNITED KINGDOM
Telephone: +44 870 600 5552
Email (orders): books.orders@tso.co.uk • (enquiries): book.enquiries@tso.co.uk • Web site: http://www.tso.co.uk

UNITED STATES OF AMERICA

Bernan Associates

4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4391, USA
Telephone: +1 800 865 3457 • Fax: +1 800 865 3450
Email: orders@bernan.com • Web site: http://www.bernan.com

Renouf Publishing Co. Ltd.

812 Proctor Avenue, Ogdensburg, NY 13669, USA
Telephone: +1 888 551 7470 • Fax: +1 888 551 7471
Email: orders@renoufbooks.com • Web site: http://www.renoufbooks.com

United Nations

300 East 42nd Street, IN-919J, New York, NY 1001, USA
Telephone: +1 212 963 8302 • Fax: 1 212 963 3489
Email: publications@un.org • Web site: http://www.unp.un.org

Orders for both priced and unpriced publications may be addressed directly to:

IAEA Publishing Section, Marketing and Sales Unit, International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 or 22488 • Fax: +43 1 2600 29302
Email: sales.publications@iaea.org • Web site: http://www.iaea.org/books

15-02211

RADIOLOGICAL CRIME SCENE MANAGEMENT
IAEA Nuclear Security Series No. 22-G
STI/PUB/1672 (93 pp.; 2014)
ISBN 978–92–0–108714–0 Price: €48.00

NUCLEAR SECURITY SYSTEMS AND MEASURES FOR THE DETECTION OF NUCLEAR AND OTHER RADIOACTIVE MATERIAL OUT OF REGULATORY CONTROL
IAEA Nuclear Security Series No. 21
STI/PUB/1613 (60 pp.; 2013)
ISBN 978–92–0–142910–0 Price: €30.00

OBJECTIVE AND ESSENTIAL ELEMENTS OF A STATE'S NUCLEAR SECURITY REGIME
IAEA Nuclear Security Series No. 20
STI/PUB/1590 (15 pp.; 2013)
ISBN 978–92–0–137810–1 Price: €20.00

NUCLEAR SECURITY RECOMMENDATIONS ON NUCLEAR AND OTHER RADIOACTIVE MATERIAL OUT OF REGULATORY CONTROL
IAEA Nuclear Security Series No. 15
STI/PUB/1488 (33 pp.; 2011)
ISBN 978–92–0–112210–0 Price: €23.00

The threat of nuclear terrorism has been recognized as a matter of concern for all States, and the risk that nuclear material or other radioactive material may be used in a criminal act represents a serious threat to national and international security, with potentially serious consequences for people, property and the environment. This Implementing Guide describes the concepts and methodologies for a risk informed approach for planning, design and implementation of nuclear security measures for nuclear and other radioactive material out of regulatory control.

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 978–92–0–100315–7
ISSN 1816–9317