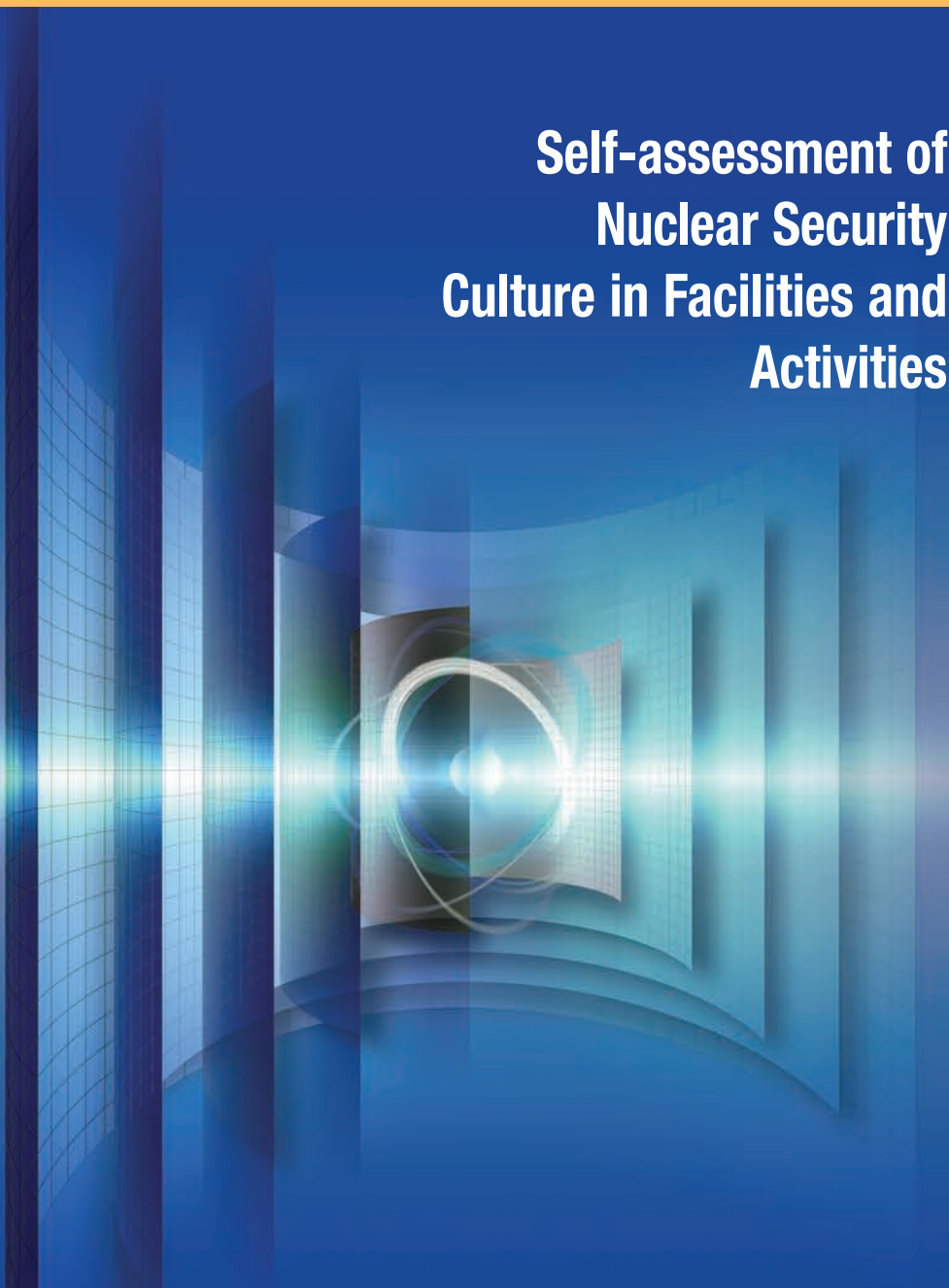
IAEA Nuclear Security Series No. 28-T

Technical Guidance

Self-assessment of Nuclear Security Culture in Facilities and Activities



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.

SELF-ASSESSMENT OF NUCLEAR SECURITY CULTURE IN FACILITIES AND ACTIVITIES

The following States are Members of the International Atomic Energy Agency:

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ANTIGUA AND BARBUDA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BAHAMAS
BAHRAIN
BANGLADESH
BARBADOS
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA, PLURINATIONAL STATE OF
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BRUNEI DARUSSALAM
BULGARIA
BURKINA FASO
BURUNDI
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
CONGO
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DJIBOUTI
DOMINICA
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ETHIOPIA
FIJI
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GUATEMALA
GUYANA
HAITI
HOLY SEE
HONDURAS
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
KYRGYZSTAN
LAO PEOPLE'S DEMOCRATIC REPUBLIC
LATVIA
LEBANON
LESOTHO
LIBERIA
LIBYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAWI
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITANIA
MAURITIUS
MEXICO
MONACO
MONGOLIA
MONTENEGRO
MOROCCO
MOZAMBIQUE
MYANMAR
NAMIBIA
NEPAL
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PAPUA NEW GUINEA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
RWANDA
SAN MARINO
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWAZILAND
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA
TOGO
TRINIDAD AND TOBAGO
TUNISIA
TURKEY
TURKMENISTAN
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VANUATU
VENEZUELA, BOLIVARIAN REPUBLIC OF
VIET NAM
YEMEN
ZAMBIA
ZIMBABWE

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. 28-T

SELF-ASSESSMENT OF NUCLEAR SECURITY CULTURE IN FACILITIES AND ACTIVITIES

TECHNICAL GUIDANCE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2017

COPYRIGHT NOTICE

All IAEA scientific and technical publications are protected by the terms of the Universal Copyright Convention as adopted in 1952 (Berne) and as revised in 1972 (Paris). The copyright has since been extended by the World Intellectual Property Organization (Geneva) to include electronic and virtual intellectual property. Permission to use whole or parts of texts contained in IAEA publications in printed or electronic form must be obtained and is usually subject to royalty agreements. Proposals for non-commercial reproductions and translations are welcomed and considered on a case-by-case basis. Enquiries should be addressed to the IAEA Publishing Section at:

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

© IAEA, 2017

Printed by the IAEA in Austria
November 2017
STI/PUB/1761

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Self-assessment of nuclear security culture in facilities and activities / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2017. | Series: IAEA nuclear security series, ISSN 1816–9317 ; no. 28-T | Includes bibliographical references.
Identifiers: IAEAL 17-01116 | ISBN 978–92–0–111616–1 (paperback : alk. paper)
Subjects: LCSH: Nuclear industry — Security measures. | Radioactive substances — Security measures. | Industrial management. | Corporate culture.
Classification: UDC 621.039:005.73 | STI/PUB/1761

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. An effective nuclear security culture depends on proper planning, training, awareness, competence, knowledge, operations and maintenance, as well as on the thoughts and actions of all people in the organization. An organization may have appropriate technical systems in place but remain vulnerable if it underestimates the role of the human factor. Considering the human factor (including as it affects the upper tier of managers and leaders) is important to effective nuclear security.

1.2. In 2008, the IAEA published an implementing guide on nuclear security culture [1]. The implementing guide defines the concept and characteristics of nuclear security culture and describes the roles and responsibilities of organizations and individuals entrusted with a function in the nuclear security regime. Since then, the IAEA has conducted many international, regional and national workshops to promote nuclear security culture and train nuclear industry personnel at all levels.

1.3. The IAEA has developed and is promulgating in this publication a comprehensive methodology for evaluating nuclear security culture in practice. When implemented by a State, this methodology will help to make nuclear security culture sustainable. It will also promote cooperation and the sharing of good practices related to nuclear security culture.

1.4. This publication is the first to contain specific guidance for assessing nuclear security culture and analysing its strengths and weaknesses in a facility or activity, or in an organization. It reflects, within the context of assessment, the nuclear security culture model, principles and criteria set out in the implementing guide [1].

1.5. Devising such a methodology poses a challenge, however, since any culture depends on intangible human characteristics such as beliefs, attitudes, values and ethics. Like traditional performance audits, security culture self-assessment can help an organization continuously learn about nuclear security requirements. This applies not only to security professionals, but to all personnel. Such self-assessment provides an opportunity for an organization to understand how culture influences security performance.

OBJECTIVE

1.6. This publication is intended for use by senior managers and nuclear security specialists in organizations operating nuclear facilities and activities using nuclear and other radioactive material to assist them in assessing the nuclear security culture in their organization as a basis for identifying ways to strengthen that culture. This guidance may also be useful for regulatory bodies or other competent authorities to understand the self-assessment methodology used by operators, to encourage operators to start a self-assessment process or, if appropriate, to conduct independent assessments of nuclear security culture.

SCOPE

1.7. The guidance in this publication describes a methodology for the self-assessment of nuclear security culture. The methodology employs a wide range of tools, including survey, interview, document review and observation. While the guidance is orientated towards self-assessment, the methodology, including the data collection techniques and indicators, could also support independent assessments performed by outside organizations or regulators.

1.8. The guidance in this publication focuses on nuclear security culture in organizations operating facilities using or storing radioactive material, and particularly those using or storing nuclear material. However, its general approach could also be used for assessing nuclear security culture in other organizations with responsibilities relating to nuclear security, such as law enforcement and border control agencies.

STRUCTURE

1.9. Following this Introduction, Section 2 describes the IAEA's concept and a model of nuclear security culture as an essential element of a national nuclear security regime. Section 3 introduces the concept and practice of self-assessment, underscores the need to assess nuclear security culture and reflects on the benefits such efforts can yield for an organization. Security culture has its own unique characteristics, which can be measured — as can any other culture — by employing certain indicators. Section 4 describes a six stage process for self-assessment and briefly summarizes the content of each stage. Section 5 reviews the available data collection tools, including survey, interview, document review and observation, and provides guidance on how to use each

tool. Section 6 outlines the procedure for reviewing and analysing the results of a self-assessment. It emphasizes that the results need to be interpreted in detail to understand what is driving staff behaviour in security related situations and to identify measures to enhance future performance. Section 7 covers the final stage of the self-assessment process when the report is assembled and shared with the organization, including the devising of a follow-up action plan to enhance the nuclear security culture. Nine appendices (I–IX) provide additional guidance on the IAEA nuclear security culture concept, indicators, the preparation of surveys, the graphical representation of survey results and the conduct of interviews, as well as the use of document review and observation.

2. DIMENSIONS OF NUCLEAR SECURITY CULTURE

THE IAEA MODEL OF NUCLEAR SECURITY CULTURE

2.1. Essential Element 12 of the Nuclear Security Fundamentals [2] — sustaining a nuclear security regime — includes: "Developing, fostering and maintaining a robust *nuclear security culture*". Nuclear security culture is defined as: "The assembly of characteristics, attitudes and behaviours of individuals, organizations and institutions which serve as a means to support, enhance and sustain nuclear security" [2]; the definition in Ref. [1] did not include 'and sustain'. The role of nuclear security culture can be deduced from the implied definition of nuclear security as

> "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*" [2].

This cross-cutting concept — explicitly or implicitly — is relevant to many different aspects of nuclear security, as shown in Table 1. Accordingly, nuclear security culture and its assessment methodology need to be universal, and to be applicable to all types of facilities and activities. Figure 1 represents the IAEA model of nuclear security culture, as set out in the relevant implementing guide [1].

TABLE 1. REFERENCES TO THE APPLICATION OF NUCLEAR SECURITY CULTURE IN IAEA NUCLEAR SECURITY SERIES PUBLICATIONS ON DIFFERENT AREAS OF NUCLEAR SECURITY

Type	Number, year of publication and title of the publication in the IAEA Nuclear Security Series	Quotation relevant to nuclear security culture from the publication
Fundamentals	No. 20 (2013) Objective and Essential Elements of a State's Nuclear Security Regime	"ESSENTIAL ELEMENT 12: SUSTAINING A NUCLEAR SECURITY REGIME… (c) Developing, fostering and maintaining a robust *nuclear security culture*" [2].
Recommendations	No. 13 (2011) Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)	"A *nuclear security culture* should be pervasive in all elements of *the physical protection regime*" [3].
	No. 14 (2011) Nuclear Security Recommendations on Radioactive Material and Associated Facilities	"All organizations and individuals involved in implementing nuclear security should give due priority to the *nuclear security culture* with regard to *radioactive material*" [4].
	No. 15 (2011) Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control	"The State should implement relevant elements of the *nuclear security culture* for the trustworthiness programme" [5].

TABLE 1. REFERENCES TO THE APPLICATION OF NUCLEAR SECURITY CULTURE IN IAEA NUCLEAR SECURITY SERIES PUBLICATIONS ON DIFFERENT AREAS OF NUCLEAR SECURITY (cont.)

Type	Number, year of publication and title of the publication in the IAEA Nuclear Security Series	Quotation relevant to nuclear security culture from the publication
Implementing Guide	No. 8 (2008) Preventive and Protective Measures against Insider Threats	"Implementing a strong security awareness programme for staff and contractors contributes to an ongoing security culture within the organization" [6].
	No. 10 (2009) Development, Use and Maintenance of the Design Basis Threat	"Such methods are likely to include assessing the operator's efforts to develop detailed adversary scenarios on the basis of the [design basis threat], to identify vital areas, develop strategies for physical protection, and to create a security culture" [7].
	No. 11 (2009) Security of Radioactive Sources	"A dynamic and effective security culture should exist at all levels of operator staff and management" [8].
	No. 19 (2013) Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme	"The State's policy should recognize the need for a strong nuclear security culture to be established and maintained as a key part of an effective national nuclear security infrastructure" [9].
Technical Guidance	No. 17 (2011) Computer Security at Nuclear Facilities	"A robust computer security culture is an essential component of any effective security plan" [10].

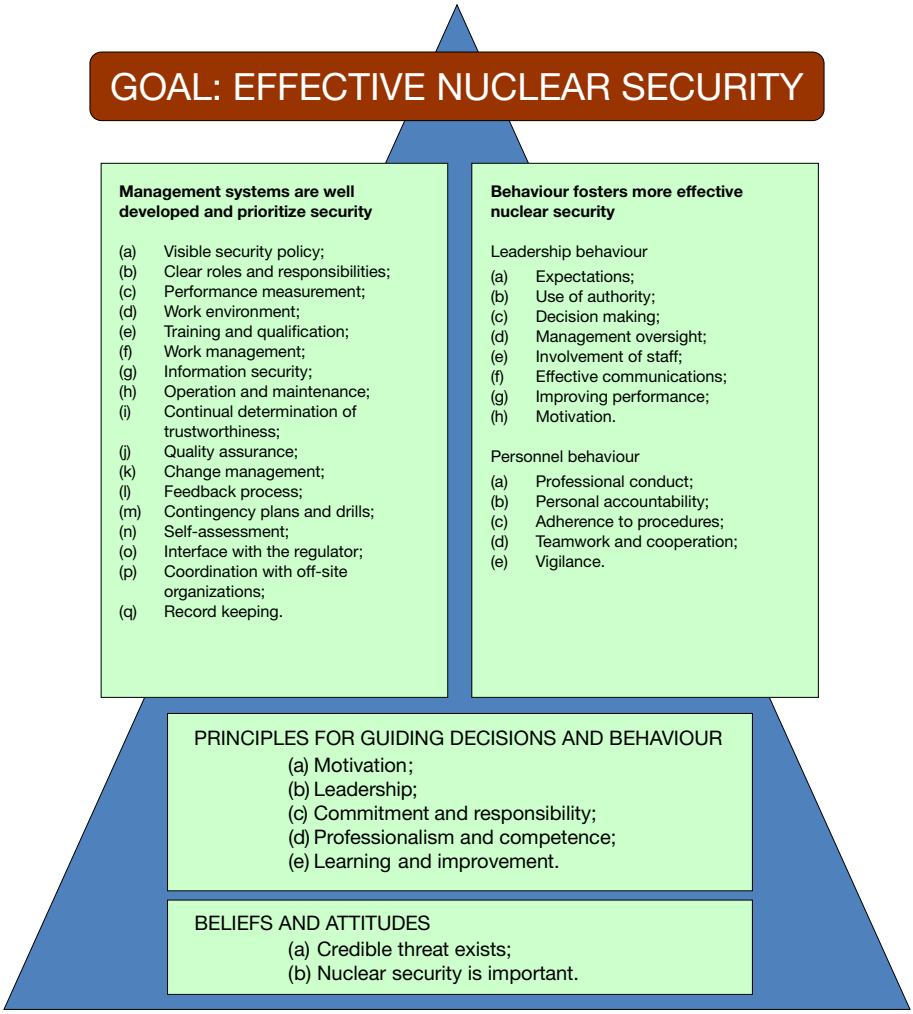


FIG. 1. IAEA model of nuclear security culture [1].

2.2. Appendix I contains a more detailed description of the IAEA's model of nuclear security culture established in the implementing guide [1] as well as of its theoretical constructs and underpinnings. The IAEA model includes 30 characteristics under the 'management systems' and 'behaviour' headings; the meaning of each characteristic is described by a set of security culture indicators in Appendix II.

INTERNATIONAL LEGAL INSTRUMENTS

2.3. Security culture is one of the 12 Fundamental Principles codified in the 2005 Amendment to the Convention on the Physical Protection of Nuclear Material [11]. The entry into force of the 2005 Amendment in 2016 made the Fundamental Principles of nuclear security, including security culture, binding on States Parties to the Convention.

2.4. The term security culture is also found in the 2004 Code of Conduct on the Safety and Security of Radioactive Sources [12]. This Code is non-binding, but more than 120 countries have informed the IAEA Director General of their support for it.

3. SELF-ASSESSMENT: CONCEPT AND PRACTICE

THE PURPOSE AND BENEFITS OF SECURITY CULTURE SELF-ASSESSMENT

3.1. The purpose of the self-assessment of security culture is to provide a clear picture of the extent to which nuclear security is part of an organization's culture. This involves evaluating the key characteristics of security culture in the organization by comparing certain indicators of the current culture with the reference levels of those indicators that would correspond to an optimal security culture.

3.2. Security culture self-assessment plays a key role in developing and maintaining an awareness of the strengths and weaknesses of an organization's nuclear security culture. By focusing on perceptions, views and behaviour at all levels of the organization, regular self-assessment helps managers to understand the reasons for an organization's patterns of behaviour in certain circumstances and to devise more effective overall security arrangements. This may be contrasted with audit type assessments, which accentuate technical issues more than intangible human elements. Self-assessment needs conscious efforts to think in terms of how individuals and teams interact with one another with the physical surroundings within the site, and with the external environment. The results of a security culture self-assessment will rarely point directly to specific technical actions, but will more typically shed light on why particular security related

issues emerge, what the root causes of problems may be and how overall nuclear security can be enhanced.

3.3. Security culture self-assessment helps both those directly involved with nuclear security and the rest of the organization by illuminating how culture influences security performance. Effective self-assessment encourages staff to accept ownership of the results and facilitates decisions that foster continuous improvement. Examples of the specific benefits of self-assessment are:

— A deeper understanding of the human factor and nuclear security culture;
— A clearer understanding of employees' concerns, needs, aspirations and motives;
— The identification of barriers to and incentives for improvements to security performance;
— The identification of barriers to and motives for change;
— The clarification of employees' opinions on security related topics;
— An improved capacity to self-assess the organization's security performance, conduct trend analysis within the site or monitor progress;
— The increased prioritization of actions that strengthen the overall organizational culture in areas such as internal communication and human resource management.

3.4. Self-assessment of nuclear security culture should complement the currently used methods for evaluating vulnerabilities and nuclear security systems, thus helping management to refine the organization's overall nuclear security arrangements.

SPECIAL CONSIDERATIONS FOR NUCLEAR SECURITY CULTURE SELF-ASSESSMENT

3.5. The idea of helping organizations to assess their own nuclear safety culture originated in the 1990s and has gained significant traction. The IAEA has issued several publications to describe and explain the self-assessment process and share good practices, such as Refs [13, 14], which were published in 2016. Safety culture assessments are also part of Operational Safety Review Team (OSART) missions. In addition, many other organizations now provide safety culture assessments: the use of external experts can compensate for a lack of in-house expertise in behavioural science, which is vital to designing assessments and understanding their findings.

3.6. As in nuclear safety, the assessment of security culture should ideally include a balance between self-assessment with and without the involvement of outside specialists, on one hand, and external assessment by a regulator or another organization, on the other, as both options have advantages and disadvantages. Self-assessment team members possess in depth knowledge of the organization, its staff, its processes and key influences. They are part of the organization and therefore have a stake in and are more accountable for improvement being made. On the other hand, staff members involved in self-assessment projects are likely to display at least some biases. There may be a need for external support and expertise to complement in-house efforts, particularly at the initial stages, and later to verify the self-assessment findings. Such external perspectives can also help managers to determine whether the necessary expertise for self-assessment is available internally.

3.7. Organizations are encouraged to develop skills related to self-assessment, including knowledge of survey protocols, interview techniques, document review, observation methods and analysis of findings. In view of confidentiality requirements in nuclear security, self-assessment is likely to be the preferred option, but a similar methodology can also be used for external assessment, i.e. independent assessment by a regulatory body or other organization if there are circumstances justifying this option.

3.8. Other particular features of security culture that need to be considered when planning and conducting self-assessment include:

(a) The overall culture of an organization being seldom homogeneous: subcultures exist within any group, and cultural analysis should therefore be open to the existence of subcultures and be ready to examine the relationship among them. An important consideration in nuclear security culture is the difference in perceptions and attitudes between security and non-security personnel. Personnel with explicitly defined responsibilities for nuclear security will understand the importance of those responsibilities, but a person who does not have such explicit responsibilities may think that security is somebody else's responsibility, and that security successes and failures have little to do with anything he or she personally does or fails to do. It is important to view security culture as the sum of these two subcultures, and understanding the differences between security and non-security personnel is vital to a balanced and appropriate assessment.
(b) That while most personnel are now accustomed to take ownership of nuclear safety, nuclear security may give rise to divergent views among the workforce. This creates challenges for the task of self-assessment. Below is

a sample list of attitudes towards security that the self-assessment team is likely to encounter over the course of a self-assessment:

— Ownership (that personnel assume responsibility, regard security as their business and feel accountable for security throughout the organization);
— Participation (that personnel adopt creative and flexible approaches towards security regulations and rules for compliance, focusing on the benefit to security);
— Compliance (that personnel follow the rules regardless of whether their compliance can contribute to better security);
— Apathy (that personnel do not care one way or another about security);
— Avoidance (that personnel regard security as inherently dangerous, unnecessary or even harmful).

(c) That since nuclear security culture aims to support and enhance nuclear security, self-assessment efforts will inevitably focus on beliefs and attitudes regarding both internal and external threats. The former pose a special challenge, and nuclear security culture, applied to the entire workforce, should be seen as a major tool to deal with the threat from insiders [15].

(d) Nuclear security at a facility having several important off-site stakeholders, and that understanding their various perceptions, beliefs and attitudes is central to effective on-site security and to teamwork among all players. These stakeholders include regulators, law enforcement agencies, off-site response forces, emergency services, trade unions and local communities. An assessment should gauge the extent to which the organization operating a specific facility or nuclear related activity has a culture compatible with that of such off-site players.

3.9. The unique features of nuclear security culture and its assessment should not separate it from safety culture: they should be complementary as parts of the overall organizational culture. Safety and security should reinforce one another in pursuing the common objective of protecting people and the environment. Leaders should promote understanding and cooperation between the two fields and a cooperative method of culture evaluation that takes advantage of their common features.

SECURITY CULTURE PERFORMANCE INDICATORS

3.10. Reference [1] assigns performance indicators to the characteristics of nuclear security culture that can be used to help assessors in measuring nuclear security culture and identifying practical ways to improve it. The main purpose of using nuclear security culture performance indicators, however, is

to stimulate thought and continuous learning rather than to prescribe specific actions. Security culture indicators constitute a framework under which change and development are facilitated, desirable behaviour promoted and undesirable behaviour discouraged. They are the main vehicles for accomplishing the goals of self-assessment and enhancement of nuclear security culture.

3.11. Use of these indicators in the self-assessment process will encourage managers to reflect upon security culture and increase their awareness of the role of the human factor in the areas being measured. Appendix II lists nuclear security culture indicators to illustrate each of the 30 characteristics of nuclear security culture included in the IAEA model. A thorough review of these indicators could be used by managers to reflect on the state of nuclear security in their organizations, identify human factor related gaps in their security systems and take corrective measures, even without undertaking a full scope self-assessment. Such simple self-reflection does not, however, preclude full self-assessment, should it subsequently become necessary to check whether the original diagnosis was correct, whether the measures adopted were effective, and whether the organization is on the right track towards enhancing its nuclear security culture.

3.12. Some organizations may regard nuclear security as a predominantly technical issue, paying little attention to the beliefs, attitudes and other cultural factors that underlie security performance. Metrics for judging the state of a culture will help broaden the thinking of people within an organization about what constitutes a good foundation for security. In the process of self-assessment, security culture indicators support four main functions:

(a) Monitoring the level of security awareness in the organization;
(b) Determining and improving tools and procedures for enhancing security;
(c) Providing a basis for developing a strategy to improve security;
(d) Motivating the management and staff to take any actions necessary.

3.13. Appendix II categorizes indicators by relevant characteristics of the IAEA nuclear security culture model. Some of the indicators are generic in nature and should be treated as examples or illustrations that each organization should tailor to its own circumstances and needs. Additional indicators should be developed, reflecting the profile of the organization and its activities. To this end, the indicators in Appendix II may be modified to address, for example, a facility's design and any special security risks, such as a surge in transport operations, extensive use of radioactive sources in the field or activities outside the established security arrangements. Self-assessment for users of radioactive sources or transport operations may need a set of specific indicators reflecting

a risk based and graded approach for such organizations. Such new specific indicators — if there is a clearly recognized need for them — should be developed by a team of experts and their use approved by management.

3.14. A security culture programme should make use of positive indicators. Positive indicators measure actions taken proactively to improve security, or to prevent security from being degraded, rather than measuring deficiencies after the fact. However, indicators cannot reveal underlying attitudes, and therefore follow-up analysis may be necessary to provide insights into how to improve. A combined use of several assessment methods can help to identify root causes and solutions.

3.15. Assessors can develop additional indicators for use in self-assessment based on specific criteria such as:

(a) The indicator being implementable and reliable;
(b) The indicator being relevant and measuring what it is intended to measure;
(c) The necessary data being available or able to be generated to provide input to the indicator;
(d) The indicator not being susceptible to bias or manipulation;
(e) The indicator being able to be easily and accurately communicated;
(f) The indicator being interpreted by different groups in the same way;
(g) The indicator being broadly applicable across the organization's operations;
(h) The indicator being able to be validated.

3.16. History, tradition and past management practices often have a lasting influence on aspects of security arrangements, and particularly on nuclear security culture. Indicators can be modified or additional indicators developed reflecting the current profile of the organization and its activities. Adjusting the indicators listed in Appendix II appropriately will help staff to perform self-assessments while encouraging stakeholders to accept the findings.

4. NUCLEAR SECURITY CULTURE SELF-ASSESSMENT PROCESS

4.1. Self-assessment is a step by step process. Initially, it may be limited to a review of indicators by the management based on available observations, document review and other sources to provide insight into the state of nuclear

security culture. If the decision is made to launch a self-assessment with a wider scope, it may be reasonable to concentrate on core characteristics relevant to the results of recent risk assessments, the conclusions of competent authorities and other sources. Analysing past security incidents and identifying their root causes may also help to select security culture characteristics that may be at risk. Limited scope self-assessment does not preclude a wider scope self-assessment if this is subsequently considered necessary.

4.2. Since the ultimate objective of security culture development is to instil such qualities of personal behaviour as professionalism, personal accountability, adherence to procedures, teamwork, cooperation and vigilance, the self-assessment may start by examining some of these qualities and their derivatives, and particularly their cultural roots. Cultural change is a long term process, in which management and staff improve nuclear security culture on a continuous basis. Security culture needs to be periodically assessed to track progress and adjust programmes, and it is beneficial to institutionalize this activity within the organization. A standing framework for nuclear security culture may include placing a senior manager in charge, periodically disseminating information about the status of security culture and preparing a core group of staff members to undertake subsequent assessments. A senior manager in charge helps strengthen nuclear security culture in general, supports the conduct of periodic self-assessments focusing on relevant culture characteristics and indicators, promotes dissemination of their results and the implementation of follow-up action plans.

4.3. The ongoing costs of the self-assessment programme should be estimated and provided for in the organization's budget. The resource costs also include time spent by employees taking surveys or in interviews away from their primary tasks and time spent by members of the self-assessment team on preparing, conducting and analysing the results of the assessment. Self-assessments should be scaled to the size of the organization, the composition of its workforce, and current and projected security risks. It may be difficult to quantify the benefits of security culture self-assessment, at least from a short term perspective, but self-assessment is an investment to achieve better nuclear security in the future.

4.4. It is essential for successful self-assessment that participation is voluntary and that the responses provided by participants are treated as confidential. The ways in which confidentiality might be breached should be carefully considered before data collection begins and explicit strategies should be put in place to avoid such breaches. The principle of voluntary participation is vital to obtain frank and sincere answers.

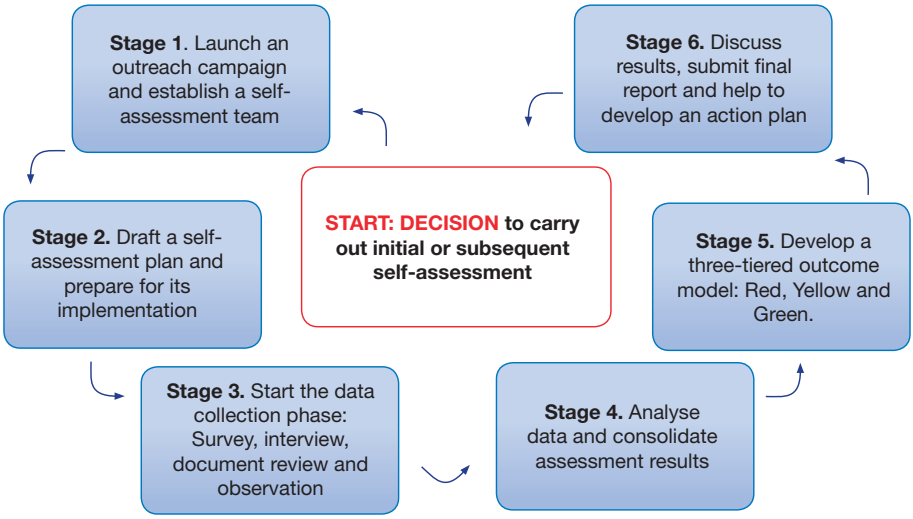


FIG. 2. The six stage process of self-assessment of nuclear security culture.

4.5. Following the preparatory work, the process has six stages, as shown in Fig. 2.

STAGE 1: LAUNCH AN OUTREACH CAMPAIGN AND ESTABLISH A SELF-ASSESSMENT TEAM

4.6. An important initial step is building commitment throughout the organization in which the self-assessment is to be carried out. Self-assessments commonly encounter problems due to misunderstanding or apathy. The organization's board and senior management should be seen to have initiated and to be supporting the process. A directive from the head of the organization is a useful vehicle for sending this message. Such a message should state the self-assessment's purpose, outline the procedure for carrying it out and explain how the results will be used. Senior management should provide visible support for the process rather than delegating responsibility. Concurrently, all senior managers should understand the scope of the self-assessment, agree to the composition of the assessment team, commit sufficient time and resources and develop a strategy to address the results of the self-assessment.

4.7. A self-assessment team is established consisting of staff members who represent different departments and who have undergone training to become familiar with the self-assessment methodology. A staff member with practical

experience in appraising nuclear safety culture would be a very helpful member of the team. The first few assessments may benefit from the involvement of an independent expert to provide advice to the team, reduce bias and share basic skills for interviewing staff members. If the national nuclear infrastructure is sufficiently extensive or diverse that more self-assessments are expected in the future, the competent authority can request the IAEA to organize a briefing or training workshop on relevant methods and procedures.

STAGE 2: DRAFT A SELF-ASSESSMENT PLAN AND PREPARE FOR ITS IMPLEMENTATION

4.8. The self-assessment team and senior management work together to develop a self-assessment plan spanning the entire process, paying due attention to the need to minimize the cost and organizational disruption. Methods to be included in the plan depend on several variables, such as the time allocated for the self-assessment, the availability of team members to perform their assessment functions, budget considerations and possible disruption of operations. These methods may be divided into two categories: non-interactive methods (surveys, document reviews and observations) and interactive methods (individual interviews, focus groups and observations). Observations are conducted both in interactive and non-interactive modes.

4.9. All these methods have their strengths and weaknesses. It is therefore recommended that a triangulated approach be used, whereby a combination of different methods is applied to the same phenomenon. Triangulation produces data drawn from multiple points of reference, but it remains somewhat subjective. All the above mentioned tools are important, but a recommended initial approach is to combine quantitative methods with qualitative methods, for example, by carrying out a survey followed by a set of on-site interviews to fill in possible gaps, clarify ambiguities and generate qualitative data.

STAGE 3: START THE DATA COLLECTION

4.10. After explaining to the organization’s staff the objectives of the self-assessment, indicating that it will focus on attitudes and behaviour, the team launches the evaluation. One possible scheme is to conduct surveys, then follow up with interviews, while at the same time accumulating relevant information from document reviews and observations. The purpose of this stage is to obtain

insight into the state of nuclear security culture and its key aspects, helping the team to determine which areas warrant further scrutiny and follow-up action.

STAGE 4: ANALYSE DATA AND CONSOLIDATE ASSESSMENT RESULTS

4.11. The team next analyses and integrates the results from surveys, interviews, document reviews and observations. While surveys, for example, provide quantitative data, interviews can capture the quality of human interactions and experiences. Comparison across the quantitative and qualitative datasets should be undertaken at the level of conclusions, not beforehand. Results that may contradict one another need to be double checked and clarified through all available means.

STAGE 5: DEVELOP A THREE TIERED OUTCOME MODEL

4.12. The next step is to develop a three tiered model of the self-assessment outcome. It could be misleading to quantify precisely the extent to which the results meet the reference levels for indicators. Instead, a simple colour coded scale of three levels can provide an adequate basis for identifying weaknesses and strengths. A green level could signify good performance, while also showing what needs to be reinforced to maintain good performance. Yellow could indicate that, despite some positive elements, certain gaps or weaknesses need to be dealt with. Red could indicate serious problems that need to be addressed as a priority.

STAGE 6: DISCUSS RESULTS, SUBMIT FINAL REPORT AND HELP TO DEVELOP AN ACTION PLAN

4.13. The team communicates the security culture profile to the management and then, with management, jointly shares its highlights with the organization, requesting feedback. In developing a follow-up action plan, it is important for management to go beyond visible behavioural symptoms to the deeper, intangible tiers of the culture that represent the causes. By identifying inconsistencies and conflicts between behaviour, practices and policies and guiding principles, beliefs and attitudes, the plan's drafters address the underlying causes of deficiencies and problems. This approach provides a basis for the organization to enhance nuclear security culture after the assessment.

4.14. After the plan has been finalized, senior management briefs the organization on its content. In addition to communicating general information to the entire workforce, they initiate specific actions designed to improve security culture. Senior management keeps lines of communication open in case any parts of the action plan need to be clarified. Follow-up assessments using a combination of old and new indicators can help identify trends while ensuring that implementation of the action plan is helping to enhance nuclear security culture. Management assigns responsibilities for implementing elements of the action plan and monitors progress on the actions. The action plan may also provide inputs into future rounds of self-assessment.

4.15. While the action plan will set out specific actions to address cultural weaknesses, other arrangements may also be needed to achieve sustainable improvement. These arrangements can include, for example:

(a) Ensuring that management systems adequately support security culture and that managers are committed to its continuous improvement;
(b) Including security requirements in recruitment, evaluation and promotion of employees;
(c) Continuing to provide training sessions and briefings on nuclear security and nuclear security culture;
(d) Including nuclear security culture issues in regular audits;
(e) Making sure that newcomers to the organization are familiar with its traditions of and requirements for security culture;
(f) Integrating security culture issues into the business planning process;
(g) Keeping the organization informed of security culture developments in other organizations and sharing good practices, if appropriate;
(h) Including performance in nuclear security and security culture in evaluations of employees and managers;
(i) Bridging safety and security culture.

5. METHODS FOR SELF-ASSESSMENT

SURVEYS

5.1. Surveys provide a convenient way to obtain input from a large number of employees. Surveys can be easy and quick to complete, helping to minimize disruption of work while encouraging a high response rate. This method can

provide clear and straightforward data because anonymous respondents can express critical views without fear of adverse consequences. Appendix III provides a step by step guide to preparing and conducting a survey.

5.2. Surveys are important in self-assessment because, in addition to quantifying current perceptions, they establish a baseline for comparisons over time. To allow such comparisons, at least some key indicators from the initial self-assessment need to be retained in subsequent surveys. Surveys also enable high level reflection on selected characteristics of security culture, helping management compare responses from different groups and strata of the organization to identify areas of strength and weakness in particular aspects of security culture.

5.3. Respondents to a survey are requested to provide comments when they mark 'neither agree nor disagree', as this indicates that a respondent feels unable to pass judgement on a particular point; respondents giving this answer are requested to provide a reason in the comment space. The comment space is particularly important because it can help to clarify data that could otherwise be subject to a wide range of interpretations. If respondents know nothing about the subject of a statement, they should tick the 'not applicable' (N/A) box. Given the large number of responses demanded in the survey, a small number of comments may simply be a result of fatigue, so care should be taken when interpreting such results.

5.4. The list of nuclear security culture indicators in Appendix II, in addition to any new ones suggested by the self-assessment team, provides the basis for statements with which respondents are asked to express their level of agreement or disagreement. While some indicators can be used directly as statements in the survey as they stand, others may need to be transformed into statements according to certain criteria (see Appendix III for specific examples). The criteria are as follows:

(a) Each statement should concentrate on a single topic. Some of the security culture indicators either reflect a combination of topics or describe a multistage process; respondents might not be able to give a single answer regarding the indicator, but the indicator may be addressed through a series of statements to which single answers can be given.
(b) Certain indicators may need to be personalized to strictly concentrate on individual attitudes.
(c) Special attention should be paid to qualifying adjectives and adverbs such as 'adequately', 'well defined' and 'reasonably', which call for respondents to exercise individual judgement. Such qualifying words may introduce

ambiguities if not clearly defined. On the other hand, they may encourage participants to provide qualitative comments that might not be made if the qualifiers were not included.

5.5. A prerequisite for regularly held self-assessments is to involve a full range of stakeholders in reasonably large numbers. The first survey provides an overall picture of the state of security culture and the basis for an action plan aimed at improving it. Since indicators can be very diverse and specialized, the first survey team needs to select metrics with which most respondents are reasonably familiar. Subsequent self-assessments may be structured differently, or may include concurrent surveys that target relevant professional groups separately; for example, separate surveys for security personnel and non-security personnel, or for managers and non-managers. Other options may be chosen to evaluate individual characteristics.

5.6. Pitfalls to be avoided when conducting surveys include:

(a) Including too many statements, causing fatigue in respondents;
(b) Providing inadequate instructions for completing the survey;
(c) Asking respondents to respond to statements on topics in which they lack necessary knowledge or background information;
(d) Failing to assure respondents that their anonymity is protected;
(e) Failing to explain the purpose of the survey;
(f) Including statements that are open to misinterpretation;
(g) Conducting a survey when staff are too busy to give it their full attention.

5.7. Piloting surveys in advance can help to reveal unclear or confusing terminology, ambiguities in questions or unjustified assumptions in the design of the survey. A pilot group could consist of 12–15 individuals, representing a cross-section of the pool of intended respondents.

5.8. Appendix IV provides a set of histograms giving a graphical representation of example survey results, and Appendix V describes a possible scheme for conducting a survey.

INTERVIEWS

5.9. Interviews play a significant role in the assessment of security culture as a source of qualitative data because they provide flexibility, allowing follow-up questions to be asked based on respondents' answers to earlier questions.

This provides a way to gain understanding of the deeper, less tangible aspects of an organization's culture. Appendix VI provides a step by step guide to conducting interviews and other relevant information. Interviews can also help management to:

(a) Obtain a differentiated view of nuclear security performance at a facility, and of activities that bear on security;
(b) Determine the extent to which staff formally and informally accept and understand security related policies, processes and procedures;
(c) Explore social norms, beliefs, attitudes and values of management and staff as they relate to security, and the relationships between important security related traits.

5.10. Interviews allow for personal interaction between an interviewer and a respondent, ideally fostering an unconstrained exchange of information. Interviewees need to be carefully selected to provide a suitable cross-section of experience, work positions and skills. Interviewees can give specific examples of practices that they have observed or heard about and this may provide clues to their insights into the beliefs and attitudes of others. Such discussion of past and current practices may be a good way to encourage interviewees to speak freely.

5.11. Face-to-face interviews can be divided into three broad types: structured, semistructured and unstructured. Structured interviews involve asking a series of closed questions and are essentially surveys completed orally. They provide few benefits compared with surveys, except for compelling respondents to take part and answer all questions.

5.12. Semistructured interviews allow the self-assessment team to investigate the context surrounding nuclear security in the organization or at the facility. For example, a general initial question might be: "What is your personal role in and contribution to maintaining or improving nuclear security in the organization?" Through positive verbal and non-verbal cues, respondents can be encouraged to present their experiences and views and elaborate on their responses. Semistructured interviews include some preformulated questions or themes, some of which may derive from a preliminary review of the survey results or from previous experience with security incidents. Interviewers may benefit from preparing an informal interview guide, listing groups of topics and questions that can be asked in different ways for different participants. This can help the interviewer to focus on the topics at hand while tailoring questions to the self-assessment goal.

5.13. Ideally, such interview guides would be continuously evolving tools in which questions are developed, tested and refined based on what is learned from asking them of different people and, perhaps, in different ways. To this end, members of the assessment team would share the results of each interview with one another prior to subsequent interviews. This cross-fertilization helps them to predict what kind of discussion might emerge when certain questions are asked and identify questions that need to be refined; to share experiences from previous rounds of interviews to improve performance at subsequent sessions; to identify future interviewees based on recommendations from past ones; and to reflect on the interviewer's role, the conditions for face-to-face interviews and the behaviours encountered during interviews, in order to make adjustments and avoid mistakes. The breadth and depth of the assessment team's experience will determine how much benefit it can derive from semistructured interviews.

5.14. Unstructured interviews do not have predetermined categories of questions or answers, and depend much more upon the skills of the interviewers. Furthermore, the results of unstructured interviews may be very diverse and difficult to interpret.

5.15. If surveys assume that people know how they feel, it often takes listening to the opinions of others in a small group setting before they can form in depth thoughts and views of their own. Focus groups are structured around a set of carefully predetermined questions, but the discussion is free-flowing. Ideally, participant comments stimulate and influence the thinking and sharing of others. Some people even find themselves changing their thoughts and opinions during the group discussion. Focus group participants are not informed of the questions prepared for discussion before the session to ensure improvisation and spontaneity. To make sure participants understand and can fully respond to the questions posed, questions should be short, to the point, each focused on one dimension, and worded in a way that they cannot be answered with a simple 'yes' or 'no', inviting participants to explain 'why' and 'how.'

5.16. Focus groups may be more effective for exploring broader security related issues. They can also yield a large amount of information within a relatively short period. Compared with individual face-to-face interviews, group discussions have the advantage that interactions within the group often prompt and sustain discussions with minimal input from the interviewer. Group members share their experiences of and views and attitudes on the topic in question, eliciting responses from one another. Because of differences in age, gender, education, access to resources and other factors, many different viewpoints are likely to be expressed by participants. The interviewer's role in such sessions is to facilitate

discussion while another self-assessment team member records key points that emerge.

5.17. Training sessions and briefings should ensure that interviewers behave appropriately, showing respect and empathy and remaining open-minded. A major challenge during interviews is to establish trust and provide credible assurances of confidentiality. If this is not achieved, there is a risk that interviewees will be selective in their responses. Efficient note taking is also a vital skill for interviewers.

5.18. Owing to the confidential nature of some nuclear security related information, it is beneficial for self-assessment teams to include individuals with appropriate clearance. The management and appropriate members of the self-assessment team will need to decide how to handle any sensitive information that arises in interviews.

5.19. Additional guidance for developing interviewing skills can be found in Appendix VI.

DOCUMENT REVIEW

5.20. Document reviews can take place prior to other self-assessment activities, to familiarize the team with past security incidents, their root causes and the corrective measures taken, or they may be used as a tool during the process of self-assessment. The primary purpose of document review is to determine whether the organization's policies and procedures provide a sufficient basis for promoting and sustaining a strong nuclear security culture. A pattern of incidents or near misses found in documents can help to narrow the focus for the self-assessment. Appendix VII provides step by step guidance on document review as a tool in self-assessment.

5.21. There are three types of document review potentially relevant to self-assessment, and the self-assessment team selects the one that best fits its needs. Such reviews may focus on:

(1) The literal meaning of documents, helping the team determine how the document's drafters intended certain work to be carried out.
(2) The interpretive meaning of documents, where the team goes beyond the document's literal wording to consider the overall context within which it was formulated.

(3) Inferences that provide wider context and an opportunity to reach conclusions well beyond the literal content of the document. For example, recurrent security breaches identified in documents and follow-up actions may point to problems with leadership, discipline, the compliance culture or the learning process. Reviewing the words in the document is necessary but insufficient to identify such deeper lessons.

5.22. Documents for review can be broken down into the following categories:

(a) Vision and mission statements;
(b) Policy statements on security;
(c) Arrangements for security, including assignment of responsibilities;
(d) Instructions for handling employee concerns, including those relating to security;
(e) Specifications of resource allocation and qualification requirements for personnel who deal with security;
(f) Security event reports;
(g) Recruitment strategies, especially in relation to security;
(h) Documentation of training activities, with special emphasis on security, including curricula, certification, rates of attendance, feedback and instructors' qualifications;
(i) Management statements, general meeting agendas and any other information deemed appropriate in the specific assessment circumstances;
(j) Records of non-compliance and related observations with potential relevance to security.

5.23. Document reviews can provide insight into how the management sets its priorities and how it intends its policies, programmes and processes to operate in practice. Combined with surveys and interviews, a document review helps the self-assessment team to appraise differences between stated policies and procedures and actual behaviour. This method also yields information about horizontal and vertical communication throughout the organization and about the efficiency of organizational learning.

5.24. A document review is a labour intensive process with administrative limitations. Before deciding to use this method, it should be determined whether the management will allow the self-assessment team access to classified documentation that might be relevant, and whether the information obtained from the review can be made available to staff and included in reports.

OBSERVATIONS

5.25. The purpose of conducting observations is to record actual performance and behaviours in real time and under different circumstances, especially training sessions and emergency drills. Observations are a well established, proven and common tool for managing security. The general principles of conducting observations include the following:

(a) The preliminary plan for observation emphasizes the most important subjects and stages of observation.
(b) Observation does not disrupt the work process and schedule.
(c) Better results are obtained through observation of the same phenomenon or action by several different observers who compare and consolidate their conclusions.
(d) Observation is systematic and draws on past observations.
(e) Previously recorded observations are often more reliable than observations made during a well publicized self-assessment campaign.

5.26. There are two basic approaches to observations as a tool of security culture self-assessment: fact based management observations and opinion based cultural observations. Observation primarily aims to identify patterns of behaviour as manifestations of beliefs and attitudes, but it is important also to monitor the completeness and functionality of the security management systems. Appendix IX provides a list of indexes to help accomplish this task. These indexes can be regularly used by managers as a checklist requiring ‘yes’ or ‘no’ answers from them. The benefit of this fact based approach to observation is that it provides specific guidance as to what to observe in the management systems that is security relevant and has implications for culture. These management system indexes enable managers to diagnose their status, identify possible gaps, take corrective action and provide guidance for more focused behavioural observation.

5.27. The opinion based cultural approach involves observing elements of culture directly (e.g. are the staff complying with procedures?) or inferring from observations (e.g. what values and beliefs do staff members express?). In this sense, observations can be used to validate findings from surveys and interviews. Cultural observations are different from observations of the performance of assigned tasks. The latter determine how consistently written policies and procedures are followed, whereas the former seek to identify cultural norms and expectations.

5.28. Cultural observations can be divided into passive and active types. The former is non-interactive and limits the observer to watching persons of interest and recording the results. The latter includes some kind of interaction, such as asking questions or requesting clarifications. Such enquiries may concentrate on specific actions or patterns of behaviour observed, such as why a particular security procedure or action was implemented and what the implications of failing to implement it would be.

5.29. An advantage of observations as a tool in self-assessment is that they do not need to be based on any underlying hypothesis that could introduce bias and distort the assessment's results. They can provide objective information and direct evidence of the truth of a given proposition, inference or conclusion. As with other methods, however, the self-assessment team should be cautious in generalizing or extrapolating from observations. Rigorous self-assessment involves the use of numerous observations of different people in different areas across the organization, helping to generate reliable information.

5.30. Observation can help not only to understand data collected through other methods (surveys, interviews and document review), but also to design questions for use with those other methods to obtain further insights into the particular phenomena being studied.

5.31. Observations made during general meetings attended by managers, staff members and contractors may provide particularly valuable insights. Questions to be answered by observation include:

(a) Do managers or the chairs of meetings refer to nuclear security requirements and expectations?
(b) Is there evidence that the staff take ownership of security? Do attendees identify issues and suggest solutions and ideas?
(c) Do staff members and contractors with security expertise actively participate?
(d) Do attendees from different professional groups express their views and interact with one another openly?
(e) Are any assumptions about risk and other security related matters questioned or confirmed?
(f) Are contributions to better security publicly recognized and praised?

5.32. Observations of other specific activities may be particularly valuable, such as:

(a) Shift changes;
(b) Routine interdepartmental meetings;
(c) Pre-task briefings by supervisors;
(d) Post-task reviews;
(e) Team meetings and project management conferences.

5.33. The observation process will be more effective if observers:

— Take notes while observing, or reserve time to take notes immediately afterwards;
— Combine formal observations of events and actions with less formal interactions with staff;
— Distinguish in their notes between simple reporting of facts and descriptions and interpretations extrapolated from direct observations;
— Regularly review their notes to synthesize different insights into particular cultural elements.

5.34. A major limitation on observations is that people commonly behave differently when being watched. Furthermore, it may be difficult to guarantee the anonymity of personnel under observation. The use of video cameras, for example, for continuous observation of a particular individual or a group is subject to national laws and internal regulations.

5.35. Further guidance on observations is provided in Appendix VIII.

6. CONDUCTING THE ANALYSIS

6.1. The analysis stage involves comparing and integrating the findings from the different assessment tools used. Without conducting such an analysis, the self-assessment team would simply be reporting what its members have been told and presenting a factual summary. Self-assessment starts as a fact based process but needs to go beyond the simple facts to be most beneficial. The significant value that team members can bring is their interpretation of the findings, their analysis of underlying root causes and their informed opinions about what problems might exist and what should be done. The organization's management can draw upon the insight of the self-assessment team to help to identify symptoms and patterns, and thereby identify underlying problems, before they lead to significant negative effects on security.

6.2. Analytical thinking is likely to enrich and contribute to the entire data gathering process, but a separate analysis stage is highly recommended. This may be short for a small organization or project, or several days may be needed to fully explore all of the issues in a large, complex organization. Participation of the entire self-assessment team in the analysis session will ensure that all members have a chance to share their views and contribute to the analysis. A preliminary analysis session, after the survey but before the team has finished gathering all the facts, will allow time for modifying interview guides, re-interviewing or adjusting interview questions to pursue issues that emerge from the preliminary analysis.

6.3. The analysis process has six steps:

(1) Organize a brainstorming session for all team members (for a preliminary or final analysis session) to identify issues that have emerged from the use of self-assessment tools. Brainstorming is intended to identify issues that may need further consideration. An original comprehensive list of all possible issues is compiled, in the expectation that this will be reduced as the process continues.
(2) Discuss the original list and revise it. Once an initial list has been established, team members discuss each issue and offer their perspectives. The conclusions reached about a particular issue may result in it being merged with others or removed from the list, and new issues may be added.
(3) Develop hypotheses to explain identified problems. Team members should look for issues that may be the root cause(s) of identified problems, consider why these issues exist, whether other means can be used to confirm their effects and how widespread they are in the organization.
(4) Review the hypotheses, test them against known information, and seek new evidence by re-interviewing relevant individuals and by other methods as appropriate. This should lead to the team confirming hypotheses that they believe to be correct, on the basis that they fit the available evidence and are considered reasonable.
(5) Formulate conclusions, explaining why each issue was identified, its cultural roots, its relevance for nuclear security and what needs to be done to address it. This outline of the conclusions is designed for inclusion in the final self-assessment report that the team will develop and submit upon completion of the analysis stage.
(6) Develop a clear, simple model for presenting the conclusions arrived at by the self-assessment team. For example, in a three colour model of red, yellow and green, red would denote identified weaknesses requiring action, yellow would denote issues that could potentially become significant

problems and green would denote strengths of the organization that need to be maintained and used to achieve the objective of more effective nuclear security. Cultural change is a slow process, and therefore it may be prudent, particularly for early self-assessment studies, to focus on just a few key items.

6.4. The two case studies presented in paras 6.5–6.9 illustrate the suggested analysis methodology.

CASE STUDY 1

6.5. In a survey, a significant number of respondents in an organization disagreed with the statement: 'Security is a clearly recognized value in the organization'. Such a response carries clear cultural implications and was selected for further analysis. These respondents apparently doubted that the existence of a threat or the importance of nuclear security were recognized, suggesting that the underlying beliefs and attitudes of nuclear security culture were not always present.

6.6. In their efforts to understand the cultural root causes of this response, the assessment team reviewed responses to similar statements and comments that might provide clues. The initial list of hypotheses included: (a) that inefficient lines of communication prevented management from delivering a clear message; (b) that the training programme placed too little emphasis on security; (c) that security arrangements were a low priority in the organization's budget, reducing its importance in the eyes of the staff; (d) that policies pertaining to career advancement ignored security performance; and several others. To reduce the list to a few working hypotheses, team members used interviews, reviewed documents and discussed their observations with managers. As a result, the self-assessment team arrived at a shorter, better validated list of hypotheses with only two remaining: inefficient lines of communication; and career advancement ignoring security performance. After further elaboration, team members agreed that because of poor coordination, messages from management about the importance of nuclear security failed to reach all groups of staff. In the absence of consistent policies and efficient use of communication channels, there was a growing trend among the staff to give nuclear security a secondary role and treat it accordingly.

CASE STUDY 2

6.7. In a survey, a significant number of respondents in an organization disagreed with the statement ‘Security is a clearly recognized value in the organization’, but a significant number of other respondents agreed with the same statement. These conflicting responses present a slightly different challenge to those described in Case Study 1.

6.8. In this case, the self-assessment team started by determining whether there was a consistent difference in perception between security and non-security personnel (although surveys were completed anonymously, respondents were requested to indicate to which general category of staff they belonged). If this hypothesis were correct, the effective existence of two subcultures could be a significant obstacle to effective cooperation between the two groups. However, the conflicting responses may have resulted from a variety of other factors and phenomena, for example, differences of perception between different non-security related departments or between long-time employees and new recruits. Yet another possible root cause specific to the organization might have been a tradition of exempting senior personnel and high ranking visitors from burdensome and time consuming security measures for access to sensitive areas. Such exemptions may send the message that senior leaders are a privileged category and care little about such security arrangements, with the implication for lower level staff that security is not important.

6.9. The initial list of possible causes therefore included the following hypotheses: (a) the existence of two conflicting subcultures of security and non-security personnel; (b) new employees being slow to adopt the organization’s culture; (c) the failure of senior management to act as role models; and (d) inefficient lines of communication. Further deliberations among team members and further interviews enabled the team to eliminate (a) and (b) from further consideration. The self-assessment team agreed that the remaining hypotheses — failure of senior management to act as role models and insufficient lines of communication — were interconnected and together could explain the differences of perception among the staff. Appropriate conclusions were drawn and reflected in the final report.

FRAMEWORK FOR ANALYSIS

6.10. Effective analysis requires an analytical framework based on interpretation. In cultural analysis, this framework needs to be made explicit and to include

knowledge of how culture operates. Information obtained from surveys, interviews and other methods needs to be interpreted and analysed to provide the basis for conclusions, rather than leaping to conclusions that might appear self-evident without such interpretation and analysis.

6.11. The three tiered model of self-assessment outcome (see Fig. 3) differs from the three colour system for presenting survey results (see Appendix III) because it represents the outcome of the entire self-assessment process. It reflects the essential nature of the security culture, emphasizing strengths (green) and weaknesses (red and yellow). After comparison and consolidation, some themes originally in one category based on the survey results may be moved to another and may require different corrective actions. Comparing the results only from a survey with those in the final three colour scheme can demonstrate how the input from other self-assessment methods can modify initial conclusions by revealing deeper cultural layers of security related successes and problems.

6.12. Self-assessment conclusions may identify numerous problems in an organization, such as overconfidence and complacency, failure of leaders to act

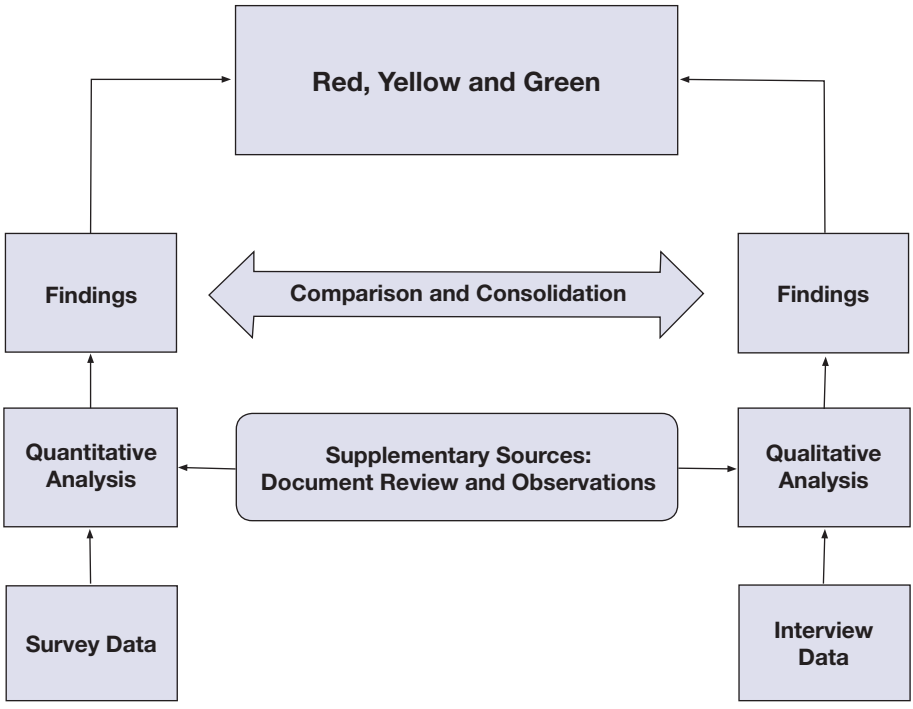


FIG. 3. Use of quantitative and qualitative data for findings analysis.

as role models, lack of a systemic approach towards security risks, leadership and management that depend more on security technology and underestimate the role of the human factor, apathy or ignorance towards security culture, and indifference to the experience of others. Consistent use of indicators as references will help the management to draw up an action plan for cultural transformation.

7. COMMUNICATION OF FINDINGS AND TRANSITION INTO ACTION

7.1. The self-assessment process leads to the compilation of a final document summarizing the results and providing the basis for communicating key messages to management and staff, a baseline for subsequent self-assessments and a starting point for the action plan. Given its wide scope and multiple purposes, the report should cover the following:

(a) Rationale for focusing on culture as a contributor to nuclear security;
(b) Reasons the self-assessment was undertaken, what methods were used and who was involved;
(c) Basic information about the way the analysis was conducted;
(d) Patterns and themes that illustrate strengths and weaknesses in the nuclear security culture;
(e) An invitation to all staff to provide feedback on these or any other items.

7.2. A major purpose in sharing the content of the report with the organization is to foster a sense of ownership among the staff. To this end, the report needs to emphasize the benefits of this long term endeavour to individuals and groups, helping them to go beyond the customary compliance based understanding of security. Benefits can include an efficient security regime, better IT security, protection of trade secrets, improved safety, reduced theft and diversion of material, reduced risk of vandalism and sabotage, improved mechanisms for control during emergencies and less need for cumbersome auditing procedures.

7.3. Communication intended to elicit feedback and advance organizational learning typically occurs in several formats:

(a) The self-assessment team conducts an exit meeting to report the review's main findings to management.

(b) Management and the self-assessment team jointly disseminate the review's findings to the staff, holding face-to-face meetings, workshops and seminars, supplemented as necessary by bulletins, information on the Intranet and social media postings. In doing this, due account needs to be taken of the confidential nature of some of the information and, if necessary, the final self-assessment report may be issued in two versions: a complete report for internal use and a version without sensitive information for the public domain.

7.4. The communication phase draws to the attention of senior management and the entire organization the role of the human factor in security, helping them to learn lessons and take corrective action. Findings should be discussed, not simply published in a report; debate can help management and staff to recognize gaps and problems in the culture that might increase the likelihood of security breaches.

7.5. The final stage in the process is for senior management to use the self-assessment results to determine how to change knowledge and behaviours that are incompatible with an effective security culture. It is especially important to eliminate any complacency that exists and avoid it in the future, by building and maintaining a robust security culture.

7.6. Figure 4 illustrates potential sources of complacency. As is the case with safety culture, overconfidence is a precursor of complacency in security culture. In both cultures, complacency is a result of good performance in the past, praise from the self-assessment team and unjustified self-confidence [15]. If it is not recognized and corrected, overconfidence can turn into complacency.

7.7. Self-assessment is designed to diagnose signs of complacency and address its root causes. It can do this by focusing on minor security events and near misses, by overcoming any tendency to ignore such events, by analysing negative (and neutral) findings from different perspectives and by evaluating the actual effects of ongoing improvement programmes, not assuming that the expected effects will occur. Periodic self-assessment can be a powerful tool to prevent sliding towards complacency and weakening of nuclear security. This can be accomplished only if members of self-assessment teams are carefully selected for their commitment and dedication and for their specific skills.

7.8. Management needs to draw timely lessons from the diagnosis provided by self-assessment and address all identified strengths and weaknesses of culture as part of its long term strategy. Management should be advised to:

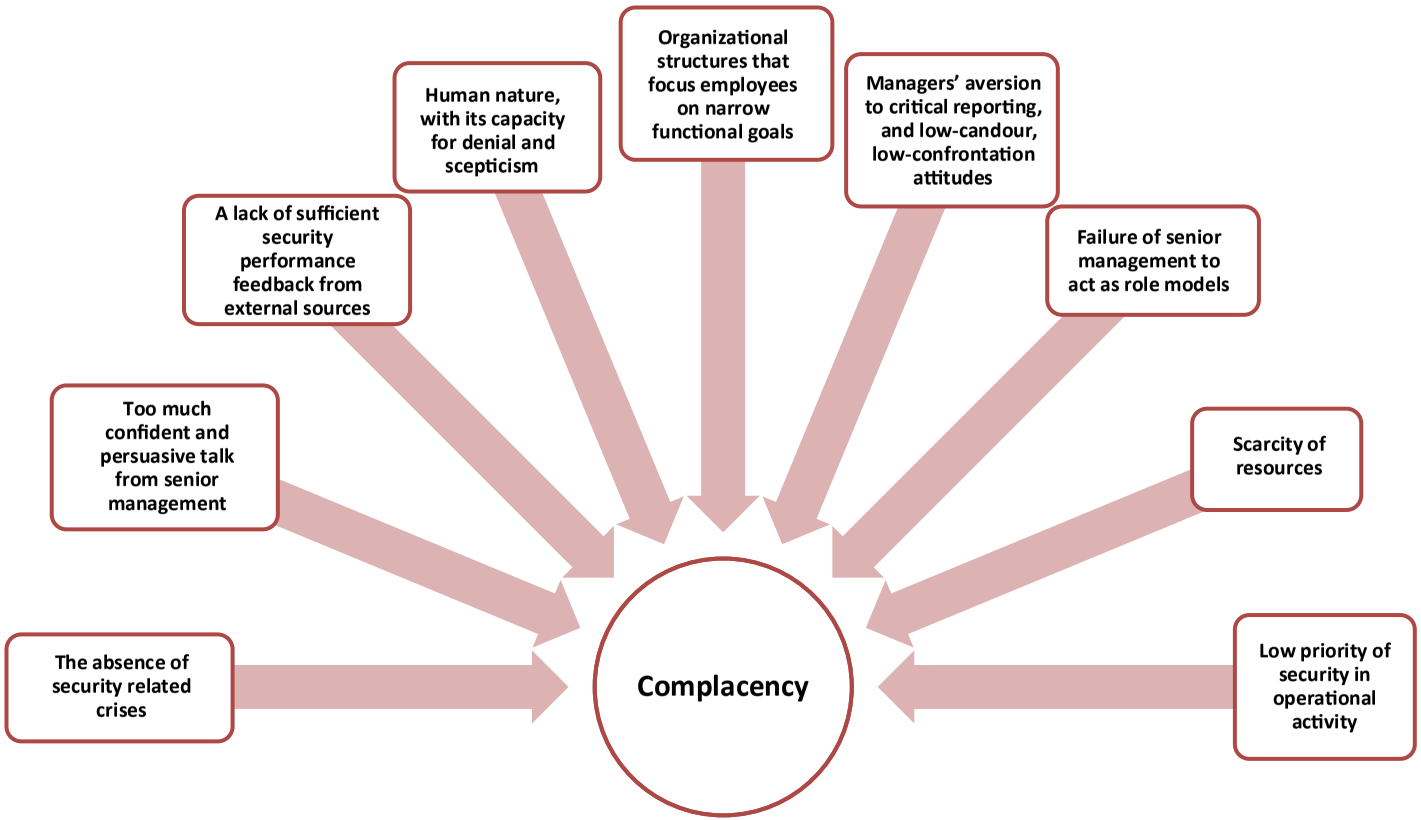


FIG. 4. Root causes of complacency.

(1) Never start with the idea of changing culture. Start with the specific issues facing the organization, and only when the problems are clear, consider whether the existing culture helps or hinders efforts to address them.
(2) Remember that culture is not an undifferentiated mass. Culture varies from endeavour to endeavour. An organization can have a culture that helps to achieve one type of result but provides little help with another. This is why nuclear security culture needs to be investigated specifically: it cannot be assumed to exist just because the facility is performing well in other respects.
(3) Think of culture as a source of strength until proved wrong. Even if some elements of the culture appear dysfunctional, remember that these may be a few weaknesses among many more strengths. If change is necessary, build upon existing cultural strengths rather than concentrating on weaknesses.
(4) Facilitate cultural change rather than creating a new culture. Managers can demand or stimulate new ways of thinking or working. They can monitor compliance. However, members of the organization will not fully adopt a new culture unless it works better and provides benefits over time.

7.9. Drawing on self-assessment as a mechanism by which to assess the effectiveness of security culture, the action plan provides a roadmap to manage the human factor and improve security related performance. Subsequent assessments are essential to monitor progress and make any necessary adjustments. However, self-assessment should remain separate from the follow-up action plan for culture enhancement, which is the responsibility of senior management and will be addressed in other guidance.

Appendix I

NUCLEAR SECURITY CULTURE AND THE IAEA MODEL

I.1. In academia, the word culture is used to explain a variety of phenomena, but there is no unanimously accepted definition of the term. Perspectives differ because culture is studied by several different disciplines, each of which has its own approach.

I.2. Organizational culture, of which nuclear security culture (like safety culture) is one of several subsets, comprises broad guidelines rooted in organizational practices learned on the job. Organizational culture encompasses values that are often taken for granted, along with the underlying assumptions, expectations, collective memories and definitions present in any organization. Both business and academic communities now acknowledge that this represents a significant factor in safety, security, performance, productivity, compliance and personnel discipline. Accordingly, several methodologies have been developed to evaluate organizational culture and track its evolution over time.

I.3. Nuclear security culture is a means to improve human performance at facilities and organizations exposed to outsider and insider threats. Most security lapses result from human failings such as low motivation, miscalculation or ignorance. However, such breaches of security among personnel result from a defective organizational culture in most cases. On the other hand, developing a more effective security culture can help to enhance overall organizational culture (including safety culture), improving performance generally. When organizations set out to address the human factor by promoting an effective nuclear security culture, they set out to cultivate habits, attitudes and traditions in this domain.

I.4. This multidisciplinary approach uses a variety of managerial, organizational, behavioural and other tools. Management need not choose between a technology centred and a human centred security design. Rather, security arises from the combination of technology, culture and people. A major objective of security culture is to facilitate human interaction with technology in security critical systems in a way that helps staff members to recognize problems, identify emerging events and anticipate patterns that might lead to a security breach. The more sophisticated security technologies and arrangements are, the more important are the people who design, operate, maintain and improve the technologies.

I.5. The IAEA security culture model is based on Schein's model of organizational culture [16], which was successfully used during the 1990s to develop nuclear safety culture. The 1986 accident at Chernobyl revealed the need for such a culture, demonstrating the results of poor human performance. There are many synergies between safety and security, two domains that overlap within the overall organizational culture. Accordingly, the safety culture model provides a ready made analytical framework for exploring and promoting nuclear security culture.

I.6. Schein defines culture as

> "a pattern of shared basic assumptions learned by a group as it solved its problems of external adaptation and internal integration, which has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems" [16].

Applied to security, a subset of organizational culture, the essence of nuclear security culture is jointly learned; relevant values, beliefs and assumptions become shared and taken for granted as a nuclear facility operates at an acceptable risk and compliance level. To paraphrase Schein, these traits become shared, sustainable and indeed taken for granted as new members of the organization realize that they bring about organizational success and so must be 'right' [17]. Schein proposes that culture exists in layers comprising underlying assumptions, espoused values and artefacts [16]. Some layers are directly observable. Others are invisible and can only be deduced from what can be observed in the organization, but these constitute the driving force for human behaviour.

I.7. Cultures stem from a first layer of underlying assumptions about reality. In practical terms, this means that an organization displays observable artefacts and behaviours that relate to what its members assume about a variety of phenomena, such as vulnerability to security risks. These assumptions or beliefs ultimately manifest themselves in tangible or observable forms, for example as documents and actions. Leaders and managers imprint these patterns of assumptions and beliefs on their subordinates, but they are often held unconsciously, never discussed and taken for granted. Hence security culture assessment needs to assess underlying assumptions on the basis of observable artefacts.

I.8. The next layer of culture is espoused values, the principles in which the leadership says it believes, and which it wants the organization to display in action. The culture manifests itself predominantly through the artefacts that make

up the third and observable layer. Physical protection equipment, staff behaviours, written documents and work processes are all visible artefacts of security culture.

I.9. Using Schein's three layers of culture, the model for nuclear security culture set out in the IAEA Implementing Guide [1] breaks the layer of artefacts of culture into three parts, giving a total of five elements (see Table 1). These are: beliefs and attitudes (corresponding to what Schein calls "underlying assumptions"); principles for guiding decisions and behaviour (corresponding to what Schein calls "espoused values"); leadership behaviour (specific patterns of behaviour and actions designed to foster more effective nuclear security); management systems (processes, procedures and programmes in the organization that make security a top priority and have an important impact on the security functions); and personnel behaviour (the product of leaders' efforts and of properly working management systems).

BELIEFS AND ATTITUDES

I.10. Beliefs and attitudes that affect nuclear security are formed in people's minds over time. Once in place, they are causal factors in both preparations and responses to security incidents. An effective nuclear security culture can only be built on a strong substructure of beliefs and attitudes about threats. Efforts to instil such beliefs and attitudes need to be carefully calibrated to reach everyone working in the facility, not just the organization's security professionals. Outreach to the local community — a potential first line of defence against external threats — is also important. Two major sources of such beliefs and attitudes are the facility's leaders and individuals' work experience. Leaders need to lead by example, to embed security related ideals within the culture, shaping the staff's mental and practical habits.

I.11. The most important assumption underlying an organization's nuclear security culture is that there is a credible threat from within and outside, and that nuclear security is important. According to Schein,

> "the essence of a culture lies in the pattern of basic underlying assumptions ['beliefs and attitudes' in the IAEA model], and after you understand those, you can easily understand the other more surface levels and deal appropriately with them" [16].

PRINCIPLES

I.12. An effective nuclear security culture needs a set of principles (Schein's "espoused values") that leaders can instil in the organization to guide policies, decision making, management systems and the behaviour of people at all levels. Individuals should fully understand and share these principles, and there should be clear evidence that they are being applied consistently across the organization. The main principles of nuclear security culture include motivation, leadership, commitment and responsibility, and professionalism and competence, as well as learning and improvement. These are all essential, but learning and improvement are key to implementing the other principles. Depending on the organization's profile and specific needs, these principles may be disseminated through a wide variety of training modules, including initial training, periodic training, ongoing programmes, ongoing assessments and quality assurance of training and trainers.

LEADERSHIP BEHAVIOUR

I.13. Leaders change culture by intervening at all levels: they can introduce new and different assumptions and patterns of thinking, they can establish new patterns of behaviour and they can change the physical environment, the use of language and the guiding principles. The culture therefore tends to reflect the intentions, specific actions and priorities of the leaders, provided that leaders understand and fulfil this function.

I.14. Because they are ultimately in charge of the security regime at an organization, leaders set the standards of behaviour and performance associated with security, and ensure that these standards are well understood and met. Other tasks for leaders are to establish a formal decision making mechanism in concert with relevant staff, provide oversight and effective communication, continuously improve performance and introduce motivational tools.

MANAGEMENT SYSTEMS

I.15. The features unique to nuclear security in the 17 management systems listed in Table 1 are: (a) visible security policy; and (g) information security. Most of the others overlap with the more generic systems that constitute the overall organizational culture but their culture indicators focus on their security content. Below are brief descriptions of each management system:

(a) A policy document should exist which states the commitment of the organization to nuclear security.
(b) All organizations clearly define who is responsible for what. It is particularly important to review and update documents and schematics depicting the responsibilities of each person when organizational change is being planned and carried out.
(c) Quantifiable measures of performance, with associated goals, are an essential tool for communicating managers' expectations and assuring that staff achieve the desired results.
(d) The work environment, including both its physical and its psychological dimensions, has a major impact on how staff members perform their tasks and comply with nuclear security requirements.
(e) An effective nuclear security culture depends upon staff members having the knowledge and skills necessary to perform their functions to the required standards. Consequently, a systematic approach to training and qualifications is critical.
(f) All work is planned and managed to ensure that nuclear security is not compromised.
(g) Controlling access to sensitive information is a vital part of the security function. Accordingly, the organization implements classification and control measures to protect sensitive information.
(h) The equipment that makes up a nuclear security system is periodically maintained, as well as occasionally modified and replaced. The intended function of the system is never compromised. If part of the system needs to be temporarily removed from service, measures are put in place to compensate.
(i) Security barriers and procedures can be defeated by insiders. Processes for determining staff members' trustworthiness and mitigating insider threats are in place.
(j) The security function demands the same degree of rigour, control and assessment as any other major programme area. Security performance is documented to earn trust and support for the organization and the people in it.
(k) Since inadequate management of change to equipment, procedures, structures and roles of personnel poses problems, the organization institutes procedures to understand, plan, implement and reinforce change as it applies to security.
(l) Processes exist for reviewing experience and applying the lessons learned to improve future performance.
(m) Contingency plans are drawn up to guide the response to malicious acts or to equipment or human failures within the facility.

(n) There is a system of self-assessment that includes assessment programmes, root cause analyses, indicators, lessons learned and corrective action tracking programmes pertaining to nuclear security and security culture.
(o) Since nuclear security typically involves regulatory and law enforcement bodies, a constructive working relationship with these institutions is therefore important to ensure that information is exchanged regarding nuclear security.
(p) Nuclear security needs frequent staff and management level communication with off-site organizations that provide medical assistance, emergency maintenance and other services.
(q) The records and relevant reports must be complete, accurate, and timely and provide sufficient information to resolve irregularities. An effective records system is updated each time an item of nuclear and radioactive material is received, transferred, relocated, processed, produced, shipped or discarded.

PERSONNEL BEHAVIOUR

I.16. The ultimate objective of security culture development is a set of desired characteristics of personnel behaviour. These include professional conduct, personal accountability, adherence to procedures, teamwork and cooperation, and vigilance.

I.17. An effective security culture will yield numerous benefits, encouraging staff to remain vigilant, question irregularities, carry out its work diligently and exhibit high standards of personal and collective accountability. It is not a panacea, but it can effectively contribute to a vibrant and robust culture across the entire workforce. It helps the organization keep pace with a threat environment in which risks are too numerous and too rapidly changing to predict, even for the most farsighted leader.

Appendix II

SECURITY CULTURE CHARACTERISTICS AND ASSOCIATED INDICATORS FOR SELF-ASSESSMENT

II.1. The objective of this suggested list of indicators is to facilitate evaluation of the characteristics of nuclear security culture at the facility or activity level by using these indicators as proxies to provide a measure of the actual characteristics. Nuclear security culture, like any culture, depends on each individual member of the organization. Each indicator below may be modified if needed (for guidance to modify indicators to create survey statements, see Appendix III), or used as is as a statement in the survey, asking respondents how much they agree or disagree with its content. As most characteristics of the nuclear security culture model overlap, so do some of their indicators. Since the choice of specific characteristics is determined by the focus of the self-assessment, some duplication and repetition of indicators across all characteristics is inevitable.

MANAGEMENT SYSTEM

Characteristic I(a): Visible security policy

II.2. A policy document is needed that states the commitment of the organization to nuclear security. This document should establish the highest expectations for decision making and conduct, and should be supported by an atmosphere of professionalism in the security field. Security culture indicators for a visible security policy are:

(1) A nuclear security policy is established for the organization, is posted in facilities and offices, and staff are familiar with it.
(2) The security function has a respected status within the organization as a whole.
(3) A staff code of conduct exists, which covers the needs of nuclear security.
(4) Staff members are familiar with the code of conduct through ongoing training and awareness sessions.
(5) Security is a clearly recognized value in the organization, and management invests adequate resources in security arrangements.
(6) Security policy is reviewed and updated regularly with participation from senior management.
(7) Processes are in place to identify the mandatory requirements relating to security.

(8) Staff members and contractors understand that adherence to the nuclear security policy is expected of all personnel.
(9) Managers are visibly interested in security and integrate it into their daily activities.
(10) Nuclear security policy is kept up to date as required.
(11) Regularly held management meetings in the organization cover significant security items.
(12) Events related to the threat environment and its potential impact on nuclear security and nuclear security policy are adequately reported to all staff.
(13) There is a well defined and widely known practice to encourage implementation of the nuclear security policy, with professional rewards or recognition directly or indirectly associated with the achievement of its goals.
(14) Staff members and contractors can cite examples from the security policy statements that illustrate their meaning.
(15) Readily accessible media (Intranet, newsletters and so on) are used to disseminate the security policy to staff members and contractors.

Characteristic I(b): Clear roles and responsibilities

II.3. Members of all organizations need a clear understanding of who is responsible for what in order to achieve the desired results. It is particularly important to review and update this responsibility system when organizational change is being planned and executed. Security culture indicators for clear roles and responsibilities are:

(1) The organization has clearly defined and documented roles and responsibilities for all nuclear security positions.
(2) Staff members understand their roles and responsibilities for nuclear security and are encouraged to seek clarification when necessary.
(3) Roles and responsibilities are adequately explained to new personnel at initial briefings, training sessions or both.
(4) Responsibility for security is assigned to a senior member of the management team, but all staff members and contractors are aware that security is a shared responsibility across the whole organization.
(5) All staff and contractors understand potential threats and the security system well enough to accept their role and responsibility relating to nuclear security.
(6) Security processes and procedures are clearly defined, so that they are easy to understand, follow and evaluate.

(7) All staff members and contractors know why they are assigned security related functions, how these functions fit into the broader picture and what impact they may have on the organization.
(8) Contractual documents clearly define contractors' roles and responsibilities in nuclear security.
(9) There is a clear understanding within the organization of the security related levels of authority and lines of communication.
(10) The overall responsibility of management for security is readily apparent.
(11) The threat against which nuclear and radioactive material should be protected (e.g. the design basis threat (DBT)) is determined and well understood by all parties involved in designing, applying and evaluating the security measures.
(12) Systems are in place to identify and make use of synergies between safety and security.

Characteristic I(c): Performance measurement

II.4. Quantified measures of nuclear security performance, with associated goals, are essential in establishing management expectations and in involving staff to achieve the desired results. Security culture indicators for performance measurement are:

(1) The organization uses benchmarks and targets in order to understand, achieve and improve performance at all levels.
(2) Performance results compared with the targets are regularly communicated to staff.
(3) Action is taken when nuclear security performance does not fully match its goals.
(4) Effective performance leading to better security is rewarded.
(5) Regulatory and independent assessments of security performance are discussed at management and other meetings.
(6) The organization actively and systematically monitors performance through multiple means, for example, through management walkthroughs, reporting of issues, indicators, trend analysis, benchmarking, industry experience reviews, self-assessments and performance assessments.

Characteristic I(d): Work environment

II.5. The physical and psychological work environment has a large impact on how staff members perform their tasks and comply with nuclear security requirements. Security culture indicators for the work environment are:

(1) The work environment is conducive to high standards of performance (e.g. standards of housekeeping, timely provision of equipment and tools).
(2) Staff are consulted about the ergonomics and effectiveness of their work environment.
(3) Texts of guides and procedures are user friendly and understandable to staff.
(4) Top managers periodically visit staffed security posts. Special attention is paid to periods of reduced activity such as back shifts and weekends.
(5) Well established procedures exist for all significant security activities.
(6) Security procedures are not regarded as an excessive burden.
(7) Feedback from staff members and contractors is requested and analysed.
(8) The work climate supports teamwork and sharing of knowledge.
(9) There is a mechanism to monitor and control overtime to prevent adverse security implications due to fatigue or other related circumstances.
(10) Procedures are regularly reviewed and updated based on staff input and performance testing results.
(11) Designers and operators of security systems ensure that security measures do not compromise safety features.
(12) The safety–security interface is managed in a risk informed, balanced way.

Characteristic I(e): Training and qualifications

II.6. An effective nuclear security culture depends on staff having the necessary knowledge and skills to perform their functions to the desired standards. Consequently, a systematic approach to training and qualifications is essential for an effective nuclear security culture. Security culture indicators for training and qualifications are:

(1) A comprehensive nuclear security training programme exists, with requirements and qualification standards established and documented and communicated to personnel.
(2) Participation in security training is given a high priority and is not disrupted by non-urgent activities.
(3) Periodic evaluation of security training programmes is conducted and revisions incorporated, as necessary.
(4) Information about the status of staff qualifications is easily accessed by those who need to know.
(5) Staff members do not perform work for which they lack the required skills and knowledge.
(6) Appropriate physical fitness criteria for security personnel are established and monitored.

(7) Top managers periodically visit training sessions.
(8) Basic security awareness training instructs all staff on proper workplace security as well as on requirements for reporting security violations.
(9) Systems are in place to ensure that procedures and practices learned in training are applied in practice.
(10) Leadership skills and good practice in security are included in training programmes for managers and supervisors.
(11) Managers are committed to providing adequate resources for effective training.
(12) Organizational values and practices require security and non-security employees to participate in refresher training to improve security related knowledge and skills.
(13) Beliefs and attitudes are considered in security training.
(14) Staff members and contractors recognize that learning is a continuous and ongoing process throughout the organization.
(15) Managers are committed to participating in nuclear security courses.
(16) Training materials include good practices and lessons learned from security breaches both at the facility and elsewhere.
(17) Staff members can provide feedback on security training.
(18) Training programmes at the organization address security conscious behaviour as a key element of professionalism.
(19) Security staff members are encouraged to share good practices with other organizations, where appropriate.
(20) The absentee rate during training sessions on nuclear security is low.
(21) Arrangements are in place to enable staff members and contractors to avoid gaps in their training if they have to miss relevant modules.

Characteristic I(f): Work management

II.7. All work should be suitably planned in order to ensure that nuclear security is not compromised. Security culture indicators for work management are:

(1) Work is planned to ensure that the integrity of the nuclear security system is maintained effectively at all times.
(2) Contingency plans are established to address foreseeable events.
(3) Staff members follow the established plans or seek proper approval to deviate from planned duties and activities.
(4) Work is planned in sufficient detail to allow staff to work effectively and efficiently (e.g. resources are matched to demands, spare parts and tools are available when needed).

(5) The interfaces between work groups are considered and addressed during planning.
(6) Cybersecurity systems are developed and maintained to ensure that they are secure, that they are accredited by an appropriate authority and are operated in accordance with procedures.
(7) Security personnel are kept motivated through the training system and incentives.
(8) Managers take action on feedback to counter negative trends in security.
(9) Minor security issues are addressed promptly.
(10) Consideration is given to synergies and conflicts between security, safety and operations in order to avoid negative impact during operation.
(11) The organization has in place written policies, rules and procedures for recruitment, appraisal and termination of employment as they pertain to security.

Characteristic I(g): Information security

II.8. Controlling access to sensitive information is a vital part of the security function. Accordingly, the organization should implement classification and control measures for protecting sensitive information. Security culture indicators for information security are:

(1) Classification and control requirements are clearly documented and well understood by staff.
(2) Clear and effective processes and protocols exist for classifying and handling information both inside and outside the organization.
(3) Classified information is securely segregated, stored and managed.
(4) Staff members are aware of and understand the importance of adhering to the controls on information.
(5) Cyber systems are maintained to ensure that they are secure, that they are accredited by an appropriate authority and are operated in accordance with procedures.
(6) Access to information is restricted to those who need such access to perform their duties, have the necessary authority and have been subjected to a trustworthiness check commensurate with the sensitivity of the information.
(7) An information and computer security function is established, funded, staffed and visible.
(8) Managers are fully committed to and supportive of computer security initiatives.
(9) A documented computer security policy covering all information carriers exists and is known to all staff.

(10) Clear and effective processes and protocols for operating computer systems have been compiled both inside and outside the organization.

Characteristic I(h): Operations and maintenance

II.9. Nuclear security system equipment will require ongoing operation, periodic maintenance and occasional modification and replacement. In all cases, it is necessary to ensure that the intended function of the system is not compromised or that if systems need to be removed from service, compensatory measures are in place. Security culture indicators for operations and maintenance are:

(1) Operation and maintenance are performed according to approved procedures and vendor schedules to ensure that design requirements are not compromised.
(2) Checklists and detailed procedures are used.
(3) Measures are taken when security equipment is taken out of service for maintenance or when breakdowns occur to compensate for the affected equipment.
(4) Operational experience of security equipment is considered vital in maintenance and in planning purchases.
(5) Conservative decision making principles are applied in making decisions about the operational reliability of security software and hardware.
(6) Operations and maintenance procedures have been established consistent with the threats from which the DBT was derived.
(7) Repair and maintenance of security equipment and hardware are performed promptly.
(8) Procedures are used effectively with no tendency to take shortcuts, even if maintenance is running behind schedule.
(9) There is a system for documenting historical data on equipment and maintenance actions that are used in the analysis of reliability and maintenance needs.
(10) There are rules in place defining and controlling maximum delay times for repairing security equipment.
(11) Resources are matched to demands so that critical spare parts and tools are available when needed.
(12) There are rules for providing compensatory measures when security equipment is out of order or being repaired.
(13) Opportunities to hold workplace forums for discussing issues of mutual interest are provided to operations and maintenance staff.

Characteristic I(i): Continual determination of staff trustworthiness

II.10. Any security barrier or procedure can be defeated with insider cooperation. Therefore, effective processes for the determination of trustworthiness and for the mitigation of insider threats should be in place. Security culture indicators for staff trustworthiness are:

(1) Documented staff and contractor screening processes are matched to the risks and threats associated with the specific employment roles and responsibilities. Screening is conducted, when appropriate, on a regular basis.
(2) The process of determining trustworthiness is capable of identifying specific security risk factors, e.g. mental illness and drug and alcohol abuse.
(3) Screening processes are rigorously followed, are subject to oversight and auditing and are required for and applied to all levels of the organization, including temporary staff and contractor personnel and visitors.
(4) Real or apparent failures of the screening processes are appropriately investigated and adjudicated.
(5) Staff members are aware of and understand the importance of trustworthiness determination.
(6) Training is provided to management and other appropriate personnel to guide them in identifying apparent high risk behavioural symptoms and in applying other similar observational and analytical skills.
(7) The screening process should address factors that might lead to degradation of trustworthiness such as substance abuse, workplace violence and criminal and aberrant behaviour.
(8) An effective insider threat mitigation programme, coordinated between all aspects of the security and operations, is in place.
(9) The process of background checks is periodically reviewed.

Characteristic I(j): Quality assurance

II.11. The security function of an organization is important and requires the same degree of rigour, control and assessment as any other major programme area. Therefore, standard quality management practices should be applied. Documented evidence of the benefits of quality management initiatives can convince personnel that quality service helps gain trust and support for the organization and the people in it. Security culture indicators for quality assurance are:

(1) Assessment processes are in place for the security function.
(2) Staff throughout the organization understand that the management system is relevant to the security function and to sustaining the nuclear security system.
(3) Security processes are prepared, documented and maintained in accordance with recommended quality assurance standards.
(4) Quality assurance measures are enforced.
(5) Quality assurance procedures are periodically evaluated against good practices for the industry.

Characteristic I(k): Change management

II.12. Many organizational problems and failures arise from the inadequate management of change. This is true of changes in equipment, procedures, organizational structures and roles or personnel. Therefore, the organization should have effective processes in place to understand, plan, implement and reinforce change as it applies to the security function. Security culture indicators for change management are:

(1) Change management processes are in place for changes that could affect the security function, whether directly or indirectly.
(2) Changes in such areas as operations, safety and security are coordinated with all potentially affected organizations.
(3) Assessments of changes are made to confirm that the desired outcomes have been obtained.
(4) Evaluations are conducted during planning of the change process to determine if the change would affect established safety and security procedures.
(5) All staff members and contractors whose security related tasks are affected by changes receive the necessary training to handle the change.
(6) There is clarity about who is responsible and accountable for carrying out security related work.
(7) Baseline standards in procedures and facility design are established, from which changes are made and documented.
(8) Before modifying or acquiring hardware, software and equipment, task analyses are performed that take human factors into consideration.
(9) Tests are conducted to ensure that replaced or modified equipment performs as expected.
(10) Before implementing changes to procedures, equipment or organizational structures that are likely to affect safety and security, a communication process is established to inform and encourage adherence.

Characteristic I(l): Feedback process

II.13. An organization that can learn from its own experience and that of others will be able to continuously improve its nuclear security performance. In order to do this effectively, processes should exist for obtaining, reviewing and applying experience from internal and external sources. Security culture indicators for the feedback process are:

(1) Processes are in place to obtain, review and apply available national and international information that relates to the security function and the nuclear security system.
(2) Processes are in place to allow and encourage members of the public as well as all staff to report abnormal conditions, concerns, actual or near miss events and, where appropriate, reward them for doing so.
(3) Reports are reviewed by management with actions taken to ensure that the organization learns from experience in order to improve its performance.
(4) Documented and established review systems for processes and procedures are in place to solicit comments and inputs from all bodies within the organization.
(5) Feedback is valued and encouraged.
(6) Dissenting views, diverse perspectives and robust discussion of pending security related issues and changes are encouraged.
(7) Staff members and contractors are requested to critically review procedures and instructions during their use and to suggest improvements where appropriate.

Characteristic I(m): Contingency plans and drills

II.14. The nuclear security system should be in a continuous state of readiness to handle security events at any time. An important element of the system is the set of contingency plans used to respond to attempted or successful malicious acts or to address a breach of protection. Appropriate and realistic drills and exercises should be conducted periodically. Security culture indicators for contingency plans and drills are:

(1) Contingency plans are in place to address the defined threats and responses.
(2) The plans are tested periodically through drills and other means to ensure that they are effective and current and that the individuals involved in using them are familiar with the plans and their roles.

(3) All security systems are tested periodically to ensure that they are functional and available when needed. Special attention is paid to systems that are not activated during normal operation.
(4) The human factor in security systems is evaluated periodically to ensure that personnel are alert and available when needed. Special attention is paid to the human factor during periods of reduced activity such as during back shifts and weekends.
(5) Contingency plans are coordinated with and linked to a relevant national strategy.
(6) Contingency plans are tested not just with on-site forces but also in coordination with off-site backup forces.
(7) Managers are trained to effectively deal with exceptional situations for which no procedures have been devised.
(8) Provisions are in place to ensure that security readiness can be temporarily tightened during times of increased threat (e.g. introduction of additional measures or reduction of access).
(9) Contingency plans are based on sound human performance principles.
(10) The organization provides adequate information on potential risks to public authorities such as first responders, the police, the military, medical facilities and environmental authorities.

Characteristic I(n): Self-assessment

II.15. There should be a system of self-assessment that includes a wide range of assessment programmes, root cause analyses, indicators, lessons learned and corrective action tracking programmes that can be used for nuclear security. Security culture indicators for self-assessment are:

(1) A self-assessment programme is documented with a plan that defines the self-assessment processes.
(2) Identified deficiencies are analysed to identify and correct emerging patterns and trends.
(3) Human factor methodologies are incorporated into problem analysis techniques.
(4) Performance is benchmarked to compare operations against national and international good practices.
(5) Operational performance is observed to confirm that expectations are being met.
(6) Corrective action plans are developed on the basis of self-assessment findings and implementation of these plans is tracked.

(7) Assessment of security systems takes into account the current DBT assessment and regulatory requirements.
(8) Staff members and contractors understand their responsibility for improvements introduced as a result of security assessments.
(9) Senior managers play a visible role in the promotion, preparation and conduct of self-assessment.
(10) Members of the organization look upon assessments, reviews and audits as an opportunity rather than a burden.
(11) There is an established procedure to continuously monitor security culture through the use of indicators to implement improvements and prevent the degradation of nuclear security culture.
(12) Managers measure the extent to which training programmes contribute to improvements in attitudes towards security culture.
(13) Staff members and contractors can give examples of senior management initiated actions that are based on the results of security culture assessments.
(14) Self-assessment results are shared to the extent possible throughout the industry as part of the exchange of good practices.

Characteristic I(o): Interface with the regulator (and law enforcement bodies)

II.16. Effective nuclear security often involves several regulatory and law enforcement bodies. A constructive working relationship with each regulatory or law enforcement body is therefore important to ensure that information is exchanged freely regarding important nuclear security matters. This involves not only the relationship between the regulatory body and the regulated organization but also policy making and other bureaucratic considerations. Security culture indicators for interface with the regulator (and law enforcement bodies) are:

(1) Information is freely and regularly exchanged between the regulatory body and the organization.
(2) Information regarding vulnerabilities and threats is mutually relayed in a timely manner.
(3) Regulatory interface roles are clearly defined and interagency processes are streamlined.
(4) Nuclear security incidents are reported to the regulator.
(5) Members of the organization fully understand the regulatory body's responsibility.
(6) Members of the organization show respect for the regulatory body, and its mission enjoys visible support and cooperation from managers.

(7) Staff members and contractors view the regulatory presence on the site positively.
(8) The operator provides to the regulatory body (or to other relevant competent authority) updates regarding security culture based on self-assessment results.

Characteristic I(p): Coordination with off-site organizations

II.17. Off-site organizations are involved in many vital functions ranging from response to incidents to providing intelligence and assistance in emergency situations.

Security culture indicators for coordination with off-site organizations are:

(1) Frequent staff and management level communication is accomplished with local and national organizations involved in nuclear security.
(2) Written agreements are in place with appropriate organizations to facilitate assistance, communication and timely response to incidents.
(3) Off-site and on-site security exercises are regularly held with lessons learned incorporated into procedures and memoranda of understanding.
(4) Contractors are aware of relevant security procedures after undergoing the relevant training prior to starting work.
(5) Outside stakeholders are consistently involved when problems are being solved and decisions are made, based on the need to know principle.
(6) There is a system for communication and cooperation with current and potential suppliers and contractors that covers security related issues.
(7) Participation in recognized courses and events (e.g. those convened by the IAEA) is encouraged and supported by management.
(8) International publications and reports covering nuclear security are available to relevant staff.
(9) The organization participates in international cooperation on nuclear security issues,
(10) Nuclear security information from international publications is made available, when possible, in a language understood by the workforce.

Characteristic I(q): Record keeping

II.18. Efficient record keeping is vital to the safe and secure operation of nuclear facilities as well as to accurate audits and assessment. Security culture indicators for record keeping are:

(1) Record keeping meets requirements to support the effective functioning of the security regime and its assessment.
(2) Records and log books are user friendly and easily accessible.
(3) Records are analysed, and there is a procedure for obtaining relevant information from current records and log books as well as from archives.
(4) There is a mechanism to protect confidential records.
(5) Log books are correctly used and reviewed by management.

LEADERSHIP BEHAVIOUR

Characteristic II(a): Expectations

II.19. Leaders should establish performance expectations for nuclear security to guide staff in carrying out their responsibilities. Security culture indicators for expectations are:

(1) Leaders have specific expectations for performance in areas that affect the nuclear security system and communicate these to staff members and contractors.
(2) Leaders ensure that resources are available to provide effective nuclear security.
(3) Leaders set an example and — as is expected from all staff — adhere to policies and procedures in their personal conduct.
(4) Leaders personally inspect performance in the field by conducting walkthroughs, listening to staff and observing work being conducted, and then taking action to correct deficiencies.
(5) Leaders demonstrate a sense of urgency to correct significant security weaknesses or vulnerabilities.
(6) Leaders are able to recognize degraded nuclear security conditions and take corrective action.
(7) Leaders visibly support the high levels of security defined in a security policy or code of conduct.
(8) Managers make their security commitment known to all staff members and contractors while ensuring that this commitment translates into daily routine.
(9) Leaders provide ongoing reviews of performance of assigned roles and responsibilities to reinforce expectations and ensure that key security responsibilities are being met.

(10) Staff members and contractors can describe how managers inspect worksites to ensure that procedures are being used and followed in accordance with expectations.
(11) Constructive feedback is used to reinforce expected behaviour.
(12) Staff members and contractors can cite examples of high expectations from senior managers regarding security.
(13) Senior managers encourage the workforce to look at other organizations or other parts of their own organization to see what they can learn from them.

Characteristic II(b): Use of authority

II.20. Management establishes the responsibility and authority of each position within the nuclear security organization. Authority should be clear and documented. Security culture indicators for use of authority are:

(1) Designated managers demonstrate good knowledge of what is expected of them, recognize and take charge of all adverse security situations or situations in which vulnerability is heightened, e.g. when the security system is degraded or when the threat level is increased.
(2) Managers make themselves approachable and allow effective two way communication, and encourage staff to report concerns or suspicions without fear of subsequently suffering disciplinary actions.
(3) Leaders do not abuse their authority to circumvent security.
(4) Managers regularly spend time observing and coaching staff and contractors at their work locations.
(5) Managers hold people accountable for their behaviour.
(6) Vigorous corrective and improvement action programmes are in place, supervised by leaders, managers and the regulatory body.
(7) Managers launch, if necessary, procedures for investigating security problems, seeking advice on the causes thereof, and on improvements to be implemented.
(8) Leaders define a strategy to bring information on the current security policy to the attention of staff members and contractors.
(9) If possible, senior managers prevent staff reductions that will affect security, despite financial restraints.
(10) Leaders provide fair treatment of subordinates, understanding that errors are unavoidable, but that security breaches must be analysed and corrective actions implemented.

Characteristic II(c): Decision making

II.21. The process through which an organization makes decisions is an important part of the nuclear security culture. Adherence to formal and inclusive decision making processes demonstrates to staff the significance that management places on security decisions, and improves the quality of decisions. Security culture indicators for decision making are:

(1) Leaders make decisions when they are warranted by the situation.
(2) Leaders explain their decisions when possible.
(3) Leaders solicit dissenting views and diverse perspectives, when appropriate, for the sake of strengthening the decision taken.
(4) Leaders do not shorten or bypass the decision making processes.
(5) Decisions are made by those qualified and authorized to do so.
(6) Security related decisions from leaders are seen as reasonable.
(7) Managers are actively involved in balancing priorities to achieve timely resolutions.
(8) Leaders support and reinforce conservative decision making regarding security.

Characteristic II(d): Management oversight

II.22. An effective nuclear security culture depends upon the behaviour of individuals, and such behaviour in turn is strongly influenced by good supervisory skills. Security culture indicators for management oversight are:

(1) Managers spend time regularly observing, correcting and reinforcing the performance of staff members at their work locations.
(2) Constructive feedback is used to reinforce behaviour expected from staff.
(3) Staff members and contractors are held accountable for adherence to established policies and procedures.
(4) Staff members and contractors are empowered to make technical decisions involving nuclear security matters.
(5) Leaders ensure that they understand the safety and security performance of their organization and take steps to maintain adequate oversight of security.
(6) Managers appreciate the importance of security culture in the accomplishment of security tasks.
(7) Managers ensure that a security conscious environment permeates throughout the organization.
(8) Managers monitor personnel's coping skills and stress and fatigue levels.
(9) Managers help to build trust and promote teamwork within the organization.

(10) Managers ensure periodic audits and updates of computer security policy and procedures.

Characteristic II(e): Involvement of staff

II.23. Performance is improved when people are able to contribute their insights and ideas. Mechanisms should be in place to support this objective for nuclear security. Security culture indicators for the involvement of staff are:

(1) Leaders involve staff members in the risk assessment and decision making processes and other activities that affect them.
(2) Staff members are encouraged to make suggestions and are properly recognized for their contributions.
(3) Staff are actively involved in the identification, planning and improvement of security related work and work practices.
(4) Staff and contractors report any problem in confidence because they know that questioning attitudes are encouraged.
(5) Systems are in place to ensure that it is easy, straightforward and welcome for staff to raise issues pertaining to potential or anticipated security related weaknesses and threats.
(6) Staff members and contractors are able to contribute their insights and ideas relating to practical problems, and mechanisms are in place to support their contributions.
(7) Plans are in place to prevent labour disputes from having an unacceptable impact on nuclear security.

Characteristic II(f): Effective communication

II.24. An important part of an effective nuclear security culture is to encourage and maintain the flow of information throughout the organization. Security culture indicators for effective communication are:

(1) Leaders ensure that communication is valued and that potential blockages in communication are addressed.
(2) Leaders explain the context of issues and their decisions when possible.
(3) Leaders visit staff members at their work locations and also conduct open forum meetings at which staff can ask questions.
(4) Leaders welcome input from staff members and contractors and take action, or explain why no action was taken.
(5) Leaders keep staff members informed on high level policy and organizational changes.

(6) Staff members and contractors are comfortable raising and discussing questions or concerns, because good and bad news are both valued and shared.
(7) Policies are in place that reinforce staff members' right and responsibility to raise security issues through available means, including avenues outside their chain of command.
(8) Leaders communicate their vision of the status of security often, consistently and in a variety of ways.
(9) Clear, unambiguous and documented definitions of the responsibilities of staff members have been communicated through established channels.
(10) The security significance of rules and procedures is clearly communicated and adequately explained to personnel.
(11) All personnel are aware of a policy of clear and unhindered communications, both upward and downward, within the organization.
(12) The system of communication is regularly tested to check that information from managers is being both received and understood by personnel at all levels.
(13) Security related communications are consistent with the confidentiality policy.
(14) Measures are taken in the organization to avoid groupthink and encourage sharing of opposing views.
(15) Processes are in place to ensure that the experience of senior staff is shared with new and junior staff members and contractors at the organization.

Characteristic II(g): Improving performance

II.25. In order to avoid complacency, an organization should strive to continuously improve nuclear security performance. Leaders should establish processes and show — by example and direction — that they expect workers to look for ways to learn and improve. Security culture indicators for improving performance are:

(1) Staff members at all levels are encouraged to report problems and make suggestions for improving performance of the nuclear security system.
(2) The causes of security events and adverse trends are identified and corrected.
(3) Analysis and follow-up of events or unusual occurrences consider not only the actual but also the potential consequences arising from each incident.
(4) When an error or event occurs, the question asked is 'What went wrong?' not 'Who was wrong?' with the focus on improvement, not blame.

(5) A process exists for all staff members to raise nuclear security concerns directly with immediate supervisors, senior managers and regulatory or other bodies.
(6) Relevant security indicators are communicated to staff members and contractors.
(7) Senior managers show that the professional capabilities, values and experience of staff are the organization's most valuable strategic asset for security.
(8) Leaders exhibit a strong commitment to establishing a 'learning organization', i.e. one that values learning from internal and external sources and commits to improving security performances as a result of this learning.
(9) Managers frequently inspect work to ensure that procedures are being used and followed in accordance with expectations.
(10) Leaders provide continuous and extensive follow-up on actions involving security related human performance.
(11) Senior managers ensure relevant information is derived from the analysis of events that can be used for improving security performance.
(12) Managers and relevant staff members are aware of good practices pertaining to national and international security.
(13) If deviations from a procedure are needed, there is an efficient and effective means to manage them correctly.
(14) Human factor specialists and psychologists are engaged with the organization.

Characteristic II(h): Motivation

II.26. The satisfactory behaviour of individuals depends on their motivation and attitudes. Both personal and group motivational systems are important in improving the effectiveness of nuclear security. Security culture indicators for motivation are:

(1) Managers encourage, recognize and reward commendable attitudes and behaviour.
(2) Managers assist in implementing the insider mitigation programme by stressing the responsibility to watch for and report unusual occurrences.
(3) Reward systems recognize staff members' contributions towards maintaining nuclear security.
(4) Staff members are aware of the systems of rewards and sanctions relating to nuclear security.

(5) Annual performance appraisals include a section on performance and efforts in support of nuclear security.
(6) When applying disciplinary measures in the event of violations, the sanctions for self-reported violations are tempered to encourage the reporting of future infractions.
(7) Performance improvement processes encourage staff members to offer innovative ideas to improve security performance and find appropriate solutions.
(8) Individuals' expertise and special skills relevant to security are recognized, used and rewarded by the organization, regardless of their formal standing within the organization.
(9) The principles used to reward good performance in security reflect those used to reward good performance in safety and operations.
(10) Leaders have taken action to make nuclear security management career enhancing.
(11) Staff members and contractors can give examples of when individuals who transmitted security related concerns or potential improvements were given public recognition.
(12) A security conscious attitude is one of the factors in approving a promotion to management levels.

PERSONNEL BEHAVIOUR

Characteristic III(a): Professional conduct

II.27. All organizations involved with nuclear security need their personnel to adhere to high standards of professionalism. Security culture indicators for professional conduct are:

(1) Staff members are familiar with the organization's professional code of conduct and adhere to it.
(2) Staff members take professional pride in their work.
(3) Staff members help one another and display professional courtesy and respect when they interact.
(4) Most staff members and contractors at all levels of the organization are actively and routinely involved in enhancing security.
(5) Staff members and contractors consider the security related aspects of their work valuable and important.

(6) Staff members and contractors have the qualifications, skills and knowledge necessary to effectively perform all aspects of their security related jobs and are provided with opportunities to improve them.
(7) Staff members and contractors are prepared to address situations that they have not encountered before and for which they have no guidance, if necessary.
(8) Nuclear security work is considered a respectable and career enhancing profession for qualified personnel.
(9) Staff members and contractors notify their co-workers when these co-workers are doing something that may adversely affect security, even if doing so is not part of their job.
(10) Staff members and contractors contribute to improvements in the training programme.
(11) Security staff members participate in professional organizations and groups, both inside and outside the facility.
(12) Papers are published and presentations are made by staff on nuclear security issues.

Characteristic III(b): Personal accountability

II.28. Accountable behaviour means that all workers know what their specific assigned tasks related to nuclear security are (i.e. what they have to accomplish by when and what results can be expected) and that they either execute these tasks as expected or report their inability to do so to their supervisor. Security culture indicators for personal accountability are:

(1) Staff members understand how their specific tasks support the nuclear security system.
(2) Commitments are achieved or prior notification of their non-attainment is given to management.
(3) Behaviour that enhances security culture is reinforced by peers.
(4) Staff members take responsibility to resolve issues.
(5) Staff members and contractors consider themselves responsible for security at the organization.
(6) Personal accountability is clearly defined in appropriate policies and procedures.
(7) Procedures and processes ensure clear single point accountability before execution.
(8) Evidence can be cited that staff members and contractors are encouraged to take advice or to seek more information when they have doubts about security.

Characteristic III(c): Adherence to procedures

II.29. Procedures represent cumulative knowledge and experience. It is important that they are followed to avoid repeating errors that have already been identified and corrected. It is also important that procedures are clear, up to date, readily available and user friendly so that personnel do not depart from the approved methods. Security culture indicators for adherence to procedures are:

(1) Staff members adhere to procedures and other protocols, such as information security controls.
(2) Visible sanctions are in place and applied to encourage personnel to follow procedures.
(3) Staff members and contractors understand the potential consequences of non-compliance with the established rules for safety and security.
(4) Managers frequently inspect work to ensure that procedures are being used and followed in accordance with expectations.
(5) The organization's instructions on security are easy to follow because they are clear, up to date, easily available and user friendly.
(6) There is a well established practice of reminding staff members and contractors about the importance of following procedures.
(7) Staff members and contractors who discover discrepancies in the implementation of security procedures promptly report them to managers.
(8) Staff members and contractors show reasonable trust in and acceptance of security procedures.
(9) Procedures are immediately available at all workstations.
(10) Staff members and contractors avoid shortcuts in implementing security procedures.

Characteristic III(d): Teamwork and cooperation

II.30. Teamwork is essential. An effective nuclear security culture can best be formed in an organization in which there is extensive interpersonal interaction and where relationships are generally positive and professional. Security culture indicators for teamwork cooperation are:

(1) Teams are recognized for their contribution to nuclear security.
(2) Staff members interact with openness and trust and routinely support one another.
(3) Problems are solved by multilevel and multidisciplinary teams.
(4) Teamwork and cooperation are encouraged at all levels and across organizational and bureaucratic boundaries.

(5) Team members support one another through awareness of one another's actions and by supplying constructive feedback when necessary.
(6) Professional groups appreciate one another's competence and roles when interacting on security issues.
(7) There are opportunities to exchange security relevant information within and between units.
(8) Team members are periodically reassigned to other teams to improve communications between teams.
(9) Cross-training between different professional areas and groups is conducted to facilitate teamwork and cooperation.
(10) There are few signs of frustration, resentment or other symptoms of poor morale within the organization that may impede cooperation among different units, particularly those in charge of safety and security.
(11) Management and staff promote and implement measures to ensure cross-pollination of ideas and to maintain security cooperation between organizational units.
(12) Staff members and contractors use a common technical vocabulary to achieve easy interactions.

Characteristic III(e): Vigilance

II.31. Security depends on the attentiveness and observational skills of staff. Prompt identification of potential vulnerabilities permits proactive corrective action. An appropriate questioning attitude is encouraged throughout the organization. Security culture indicators for vigilance are:

(1) Staff members notice and question unusual indications and occurrences and report them to management, as soon as possible, using the established processes.
(2) Staff members are attentive to detail.
(3) Staff members seek guidance when unsure of the security significance of unusual events, observations or occurrences.
(4) Staff members and contractors believe that a credible threat exists.
(5) Staff members and contractors are trained in observation skills to identify irregularities in security procedure implementation.
(6) Staff members and contractors are aware of a potential insider threat and its consequences.
(7) Staff members and contractors avoid complacency and can recognize its manifestations.
(8) Staff members and contractors accept and understand the need for a watchful and alert attitude at all times.

(9) Staff members and contractors feel safe from reprisal when reporting errors and incidents.
(10) A policy prohibiting harassment and retaliation for raising nuclear security concerns is enforced.
(11) Staff members and contractors make decisions and take actions consistent with their responsibilities if a decision needs to be made before managers arrive on scene.
(12) Staff members and contractors notify management of any incidents or possible incidents involving a compromise of computer security or information security.

Appendix III

PREPARATION AND CONDUCT OF SURVEYS

III.1. Self-assessment surveys have the following advantages as a self-assessment method:

— They offer easy administration and low cost for data collection from a large number of people.
— There is a reduced likelihood of evaluator bias because the same questions are asked of all respondents.
— Surveys are a commonly used method and many people are familiar with them.
— Some people feel more comfortable responding to a survey than participating in an interview.
— Processing of responses is straight forward.

However, their limitations must also be considered:

— Those invited to respond to the survey may not complete it, resulting in low response rates.
— Items may be understood differently by individual respondents.
— Some participants may have insufficient information to respond.
— The inability to identify respondents personally and probe for additional information.

Before launching a survey, the self-assessment team should consider the benefits that this evaluation tool can bring. The following subsections give a step by step description of conducting a survey.

STEP 1: TOPIC SELECTION

III.2. A survey is usually the first major step in the self-assessment process, and it is designed to concentrate on characteristics that are believed to be weak and vulnerable, which are identified as the ‘topic’ for the survey. Such a focused self-assessment is likely to result from recent risk assessments, intelligence reports, audits, observations of senior management or security personnel or records of past security events. The selection of the topic should be made by senior management, in consultation with the security staff and in coordination with appropriate national authorities. The topic is selected prior to the survey but

its choice determines not only the survey preparation but also the use of other assessment methods.

III.3. Culture self-assessment is about human behaviour and its root causes. Hence, the focus of such a probe is on the characteristics of personnel behaviour as outlined in the IAEA nuclear security culture model: professionalism; personal accountability; adherence to procedures; teamwork and cooperation; and vigilance. The content of each of these characteristics is clarified by security culture indicators in Appendix II, grouped under each characteristic. For the purpose of the example in this appendix, 'adherence to procedures' has been selected as the topic of the hypothetical survey.

STEP 2: SELECTION OF SECURITY CULTURE PERFORMANCE INDICATORS

III.4. Appendix II lists eight indicators for the 'adherence to procedures' characteristic that need to be carefully considered for possible inclusion in a survey where this characteristic had been chosen as the topic. Consideration should be given to which of them are consistent with the nature of the organization's operations and will therefore be understood by potential respondents, and whether any additional new indicators should be developed. Indicators belonging to other characteristics in the personnel behaviour segment may also be deemed relevant and selected for the survey because of overlaps between some characteristics. Consideration should then be given to whether to include further indicators for the characteristics of 'management systems' and 'leadership behaviour'. The criteria for their selection are the extent to which they contribute to and shape personnel behaviour, helping achieve optimal security culture in the target area. Since 'adherence to procedures' is the self-assessment target, it will be necessary to review in these two segments the indicators for such characteristics as 'clear roles and responsibilities', 'performance measurement', 'training and qualifications', 'information security', 'use of authority', 'management oversight' and 'motivation'. As a result, the total number of selected security culture indicators for the survey may be between 25 and 35.

STEP 3: TRANSFORMATION OF INDICATORS INTO SURVEY STATEMENTS

III.5. Some indicators are included in the survey as they stand, but others may need modification for clarity and to conform to the specific nature of the organization. In transforming indicators, the following criteria are to be observed:

(a) Statements should have a single focus. Some, if not most indicators either have multiple focuses or describe a multistage process and are therefore statements to which respondents cannot give a single answer. Hence, it is helpful to select one element of the indicator most relevant to 'adherence to procedures' as the focus of the statement. For example, indicator I(b)(2) — "Staff members understand their roles and responsibilities for nuclear security and are encouraged to seek clarification when necessary" — was transformed into the following survey statement: "Staff members are encouraged to seek, when necessary, clarification regarding their roles and responsibilities for nuclear security."

(b) Since indicators apply to the entire organization, their full evaluation may depend on in depth background information that most respondents may lack, and so certain indicators may need to be personalized to focus on individual attitudes. Accordingly, indicator III(c)(5) — "The organization's instructions on security are easy to follow because they are clear, up to date, easily available and user friendly" — can be changed to a survey statement reading: "It is easy for me to follow instructions for security because they are clear, up to date, readily available and user friendly." Expressions of personal views requested from respondents could facilitate the search for cultural root causes. However, each survey must maintain a balance between generic (organizationwide) and personalized statements. Inclusion of selected generic statements makes it possible to understand how an individual respondent evaluates other people's behaviour and organizationwide management practice.

(c) When transforming indicators into survey statements, special attention needs to be paid to the use of such qualifying adjectives as 'adequately', 'well defined', 'reasonably' and others, which compel respondents to exercise judgement, with possible unexpected consequences. On one hand, such qualifying adjectives may confuse respondents, but on the other they may help them to provide more pertinent comments leading to valuable insights that clarify the cultural dimension of nuclear security.

(d) It is recommended to use only positive survey statements.

III.6. More examples of such transformations are given in Table 2.

TABLE 2. TRANSFORMATION OF SECURITY CULTURE INDICATORS INTO SURVEY STATEMENTS

Security culture indicator		Survey statements
Staff members and contractors who discover discrepancies in the implementation of security procedures promptly report them to managers (III(c)(7))	→	If I discover discrepancies in the implementation of security procedures, I promptly report them to management
Staff members and contractors show reasonable trust in and acceptance of security procedures (III(c)(8))	→	Members of my team show trust in and acceptance of security procedures
Staff members understand their roles and responsibilities for nuclear security and are encouraged to seek clarification when necessary (I(b)(2))	→	Management encourages me to seek, when necessary, clarification regarding my role and responsibility for nuclear security
Leaders personally inspect performance in the field by conducting walkthroughs, listening to staff and observing work being conducted, and then taking action to correct deficiencies (II(a)(4))	→	I have witnessed our leader(s) personally inspect performance in the field by conducting walkthroughs, listening to staff and observing work being done

STEP 4: SCORING SCHEME DEVELOPMENT

III.7. The self-assessment team needs to determine the scoring scheme for the survey. There are numerous options, and choosing from them should take into account past surveys and methods used, compatibility with surveys in other organizations, the management's preferences for complexity or simplicity — especially if this is a pilot project — and other factors. This publication suggests a scoring system employing a 7 point scale from 1 ('strongly disagree') to 7 ('strongly agree'). This scheme (see Fig. 5) indicates that a particular indicator is either fully observed or present, completely unobserved and absent, or somewhere in between. 'Somewhat disagree' and 'somewhat agree' provide more flexibility for respondents. 'Neither agree nor disagree' indicates that a respondent feels unable to pass judgement on a particular point, and respondents giving this answer are requested to provide a reason in the comment space. The comment space is particularly important because it can help to clarify data that could otherwise be subject to a wide range of interpretations. If respondents know

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree (explain why)	Somewhat agree	Agree	Strongly agree
1	2	3	4	5	6	7
Survey Statement						
Please write any other comments at the bottom of the page.						
	Not applicable					

FIG. 5. Seven point scoring scheme for self-assessment.

nothing about the subject of a statement, they should tick the 'not applicable' (N/A) box.

III.8. Other scoring options are possible. One is an 11 point scale from 'fully disagree' (0) to 'fully agree' (10), as shown in Fig. 6. Its application will produce more nuanced responses from the target group. As with the 7 point scale,

Fully disagree										Fully agree
0	1	2	3	4	5	6	7	8	9	10
Survey Statement										
Please write any other comments at the bottom of the page.										
	Not applicable									

FIG. 6. Eleven point scoring scheme for self-assessment.

respondents with no knowledge of the subject matter are asked to check the 'not applicable' (N/A) box.

STEP 5: AVERAGING AND GRAPHICAL REPRESENTATION

III.9. To calculate the results of the survey for each statement, all scores should be summed and divided by the number of respondents, excluding those who marked the N/A box. A colour code is applied, based on this average score. If the average score for a statement falls on the 'disagree' side of 'neither agree nor disagree' (i.e. below 4) on the 7 point scale, it is a sign of a weakness (red). If the average is within the range covered by 'neither agree nor disagree' and 'somewhat agree' (i.e. between 4 and 5), there are grounds for concern (yellow) because the current situation falls short of the standards outlined in the survey statements. The 'agree' and 'strongly agree' entries (above 5) signify strong points that should be preserved and reinforced to maintain security culture. (On the 11 point scale, average scores from 0 to 4 belong to the red segment, 5 to 7 to the yellow segment, and 8 to 10 to the green segment.)

III.10. Once red, yellow and green ratings have been assigned, the next step is to identify subgroups within each colour code or across the colour codes that appear to represent convergent or conflicting views among the respondents. Each subgroup merits special scrutiny, whether they represent predominantly negative, predominantly positive or conflicting views. Subgroups appearing in different colour codes for the same statement is an indication that the workforce is split on an important issue of nuclear security. As the self-assessment team identifies convergent or conflicting views, taking account of comments from respondents, it formulates themes for further exploration with the help of qualitative data from interviews. They may also seek input from a document review or from firsthand observations. Appendix IV illustrates how survey results can be graphically represented to facilitate self-assessment.

III.11. Understanding the strengths of a culture is as important as identifying gaps and deficiencies, and any effort to introduce a cultural change needs to take account of both. The colour coding system allows for clear recognition and strong distinctions, and provides a basis for further investigation using other self-assessment methods. Survey results are easier to manage, analyse and store if the score averaging for each statement is graphically represented as histograms; these aggregate the individual responses for each survey statement. See Appendix IV for more information on histograms.

III.12. The designated respondents (e.g. 40–50% of the main workforce including staff and contractors) are notified of the scheduled survey and members of the self-assessment team are assigned to specific individuals to explain in an appropriate format why they have been selected, the rationale and procedure for the survey and the subsequent use of the information to be collected. One option to launch the survey is to print copies of the form, keep them in an allocated conference room and invite respondents to come at a designated time to complete them. Other options for filling out the survey form, including electronically, are possible. A major problem during a survey is to focus respondents' attention on individual statements and clarify their meaning. One way to do this is to project on a screen one statement after another, providing enough time between each question to select the appropriate box for each and clarify, if appropriate, their meaning. The time needed to complete a form, scoring 25–35 statements and providing several comments, is estimated to be 40–60 minutes (depending on the language proficiency of respondents if the statements are not in their first language). Respondents are asked to place their completed forms into sealed boxes to provide additional assurance of anonymity. This procedure is ideally performed within one day (with respondents divided into groups, but for a larger number of respondents, this can be extended to two or more days). Each respondent is expected to receive a thank you note from management for participating in the survey.

Appendix IV

USE OF HISTOGRAMS TO PRESENT SURVEY RESULTS

IV.1. Survey results may be easier to manage, analyse and store if the score averaging for each statement is graphically represented as a histogram. These charts aggregate the individual responses for each survey statement along with comments from respondents. Figure 7 is a sample of a right skewed distribution, reflecting predominately positive views in response to a specific statement. This distribution is a clear signal that the performance covered by these statements is rated by most respondents as consistent with relevant culture performance indicators. These views may represent assets that should be emphasized in post-assessment outreach and used as leverage to address weaknesses. If comments exist on this statement, they can be attached to the histogram to provide additional insights into the cultural root causes of this problem.

IV.2. After plotting individual histograms for responses to all survey statements, the self-assessment team will benefit from visualization, comparison and prioritization, the three important ingredients needed to develop relevant themes for interviews. A left skewed distribution sends a message that performance is weak and appropriate measures are needed in the follow-up action plan. The survey results, however, are just one step in the multistage self-assessment process. Even if the survey outcome is predominately positive, the self-assessment team should not reach premature conclusions, because surveys represent visible manifestations only and may fail to reflect deep layers of culture. Other self-assessment methods may contradict some survey results and help identify hidden problems.

IV.3. Conflicting views divided between negative and positive responses are represented by bimodal (double peaked) histograms. Figure 8 illustrates how these views may be distributed on the 7 point scale. Such cases warrant special attention as possible indicators of cultural flaws and need to be analysed when developing an interview guide. Of particular importance is the comparative size of this division, judged by the number of points in each peak. The nature of this division should be explored during interviews. Yet another shape at which the self-assessment team may arrive is a multimodal distribution, with several peaks on both sides of the ‘neither agree nor disagree’ point. This can signify a multidimensional split in the security culture.

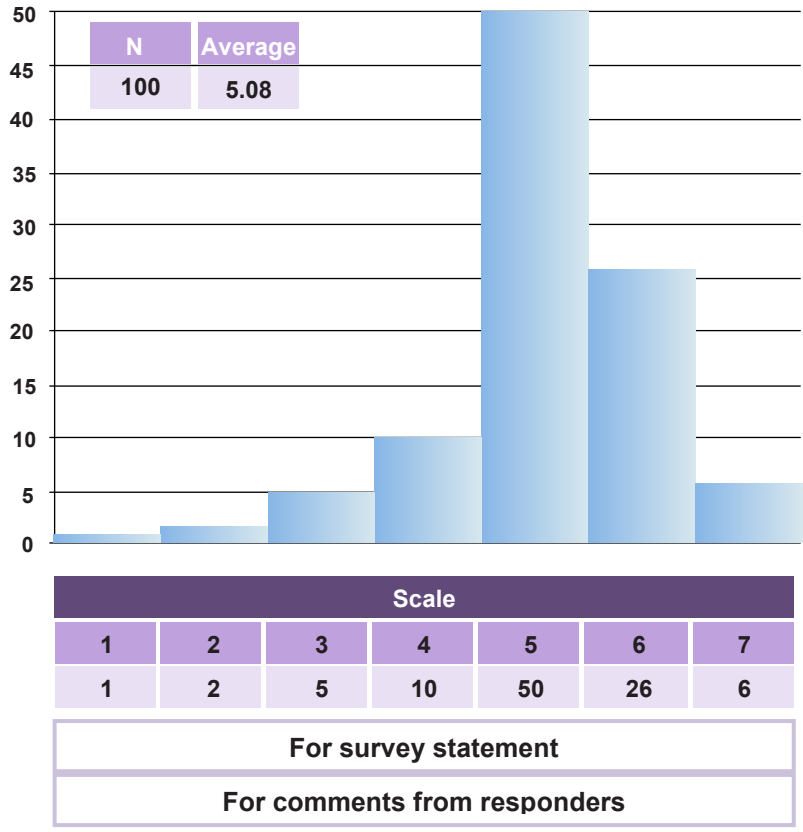


FIG. 7. An example of post-survey graphical representation of convergent views.

IV.4. Survey histograms should be archived and revisited in the process of continuous self-assessment. They will help chart and interpret the evolution of the organization's security culture over the longer term and check the effectiveness of specific management tools. Hence, it is important to include in periodic surveys several previously used statements in order to track key cultural trends and avoid human factor risks. At the same time, plotting and interpreting histograms requires special skills from members of the self-assessment teams. They should be trained accordingly, or external experts invited to carry out this task.

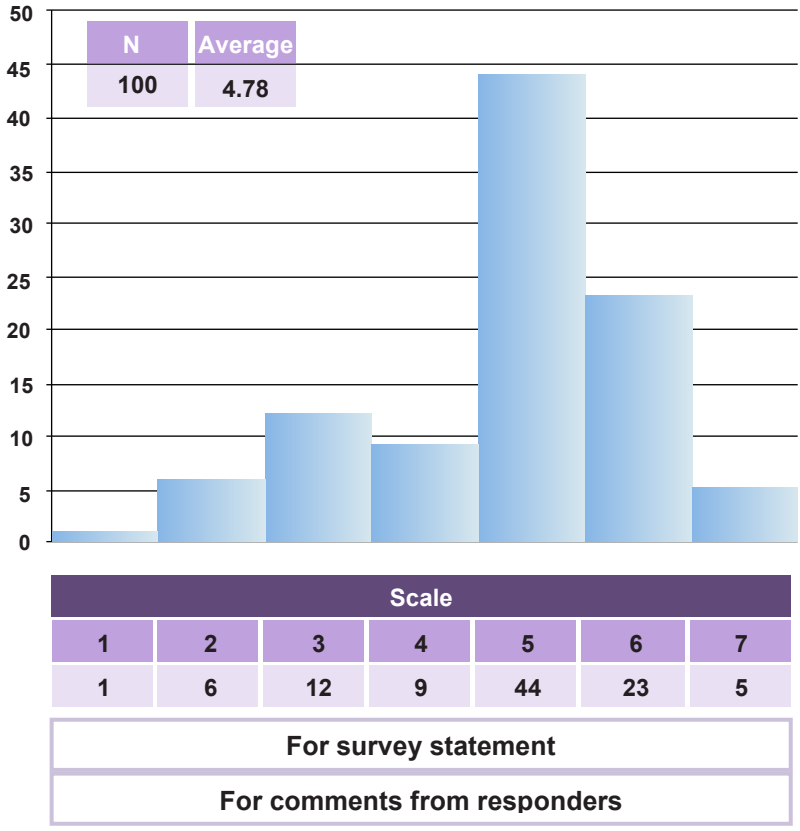


FIG. 8. An example of a post-survey graphical representation of conflicting views.

Appendix V

A POSSIBLE SURVEY SCHEME

V.1. This appendix provides a hypothetical scheme for conducting a self-assessment of security culture at a generic organization. It could be a nuclear fuel cycle facility, a research reactor, a radioactive source manufacturer or user, a transport company or any other entity within the scope of the assessment methodology. In this hypothetical example, it is supposed that a routine audit at the organization has provided evidence that the work performance of its personnel has serious deficiencies in compliance discipline. These deficiencies are supposed to have been identified in several parts of the organization, and to threaten to undermine the organization's security and safety record.

V.2. At its regular meeting, the management team discussed the audit results and possible implications of not taking corrective measures, including a change in what seemed to be a prevailing lack of compliance culture. A senior manager responsible for security reported observing signs of complacency and inadequate compliance for some time, but the actions he had taken thus far had failed to yield significant changes to the pattern of behaviour. The management team agreed that a solution to this problem lay in identifying the cultural root causes of deficient compliance, and thus that a carefully calibrated self-assessment of this aspect of the organization's security culture was warranted.

V.3. A five person self-assessment team was established by senior management and followed the step by step procedure recommended in this publication. A key task was to define the scope of the self-assessment process and develop a survey as the first step. It was suggested that the key characteristic of the organization's security culture to be reinforced is 'adherence to procedures', as outlined in the IAEA nuclear security culture model. This characteristic is to be found in the Personnel Behaviour segment of the IAEA model and has eight indicators, listed in Appendix II. These indicators were used as survey statements and respondents were requested to determine the extent to which they are present in the organization. This determination was to be made on a scoring scheme based on a 7 point scale ranging from 'strongly disagree' (1) to 'strongly agree' (7). Only positive survey statements were used, such that disagreement with the statement would tend to indicate a weakness in security culture. Scoring schemes based on fewer or more points on the scale were discussed, but the seven point scale was selected because the organization had good experience with using it in past surveys. The scheme used the responses to each survey statement to conclude whether the particular indicator associated with that survey statement is either

both fully observed and present; completely unobserved and absent; or present in part.

V.4. The survey also included indicators from the Management Systems and Leadership Behaviour categories of the IAEA model, which are designed to contribute to and shape personnel behaviour, helping achieve optimal security culture in the target area. As some characteristics overlap, so do their indicators.

V.5. The self-assessment team recognized that the list of indicators in Appendix II provides a set of benchmarks to illustrate how each characteristic should ideally evolve in pursuance of an effective nuclear security culture. Members of the team selected relevant indicators to serve as a basis for developing survey statements to which respondents were expected to express their agreement or disagreement. In transforming certain indicators into survey statements, they were guided by the criteria outlined in Step 3, Appendix III. Figure 9 shows the survey introduction prepared by the self-assessment team and Fig. 10 shows an example question as it would feature on the survey. The complete list of questions is as follows:

(1) I am aware of the nuclear security policy at my organization to the extent that I can specifically cite its provisions relevant to my job.
(2) I have become familiar with the code of conduct through ongoing training and awareness sessions.
(3) Media based communication systems (Intranet, newsletters, others) are used in my organization to disseminate the security policy to staff members and contractors.
(4) Processes are in place to identify the mandatory security requirements assigned to me.
(5) Management encourages me to seek, when necessary, clarification regarding my role and responsibility for nuclear security.
(6) I know how my security related functions fit into the broader picture at my organization.
(7) I regularly receive performance results compared with the targets.
(8) Action is taken by management when nuclear security performance does not fully reach its goals.
(9) I find the text of security related guides and procedures user friendly and understandable.
(10) I do not regard the procedures for activities significant to security as overburdening.
(11) I have been instructed during basic security awareness training on requirements for reporting security violations.

(12) Systems are in place to ensure that procedures and practices I learn in training are applied in practice.
(13) I am aware of documented actions by senior management on negative trends in security.
(14) I am aware that quality control measures are adequately enforced in the security area.
(15) Processes are in place to allow and encourage members of the public as well as all staff to report abnormal conditions, concerns and actual or near miss events.
(16) I can describe how management encourages staff members and contractors to critically review procedures and instructions during their use.
(17) I can provide examples of how operational performance is observed to confirm that expectations are being met.
(18) Our leaders lead by example and — as is expected from all staff — by adhering to security policies and procedures in their personal conduct.
(19) I have witnessed our leaders personally inspect performance in the field by conducting walkthroughs, listening to staff and observing work being carried out.
(20) Managers demonstrate how their security commitments are translated into their daily job.
(21) Managers spend time improving our security related performance by coaching my team members and me at our work location.
(22) I am aware of vigorous corrective and improvement action programmes that are effectively managed by our leaders.
(23) Management holds my colleagues and me accountable for our behaviour.
(24) I can provide examples of how management ensures that a security conscious environment prevails throughout the organization.
(25) Staff members and contractors are held accountable for adherence to established policies and procedures.
(26) Our organization has in place written policies, rules or procedures for recruitment and termination of employment as they pertain to security.
(27) Management regularly explains to me the importance of professionalism in the accomplishment of security tasks.
(28) Leaders communicate their vision of the status of security in a variety of ways.
(29) I know that there are documented definitions of the responsibilities of staff members regarding security.
(30) The security significance of various rules and procedures has been clearly and adequately explained to me.
(31) Analyses of events or unusual occurrences consider the potential consequences arising from each incident.

(32) Human factor specialists and psychologists are engaged with the organization.
(33) Security performance indicators that are relevant to my work are communicated to me.
(34) I am aware of the systems of rewards and sanctions relating to nuclear security.
(35) I am aware of cases in which a security conscious attitude has been a significant factor in a promotion.
(36) I am prepared to notify my co-workers that they are doing something that may downgrade security, even if it is not part of my job.
(37) I consider myself personally responsible for security at the organization.
(38) The concept of personal accountability is clearly defined in appropriate policies and procedures.
(39) Procedures and processes exist to ensure clear single point accountability before execution.
(40) I recognize the importance of adhering to procedures and other protocols, such as information control.
(41) Visible sanctions are applied to encourage personnel to follow procedures.
(42) When I discover discrepancies in the implementation of security procedures, I promptly report them to management.
(43) Managers frequently inspect my work to ensure that procedures are being followed as expected.
(44) It is easy for me to follow instructions on security because they are clear and user friendly.
(45) Procedures are immediately available at my workstation and at others.
(46) There is a well established practice to remind staff members and contractors through appropriate channels about the importance of following procedures.
(47) Members of my team show trust in and acceptance of security procedures.
(48) There are sufficient exchange opportunities for security relevant information within and between units.
(49) I have been involved in cross-training in different professional areas and groups conducted to facilitate teamwork and cooperation.
(50) My team members and I are periodically reassigned responsibility to improve interteam communications.

Survey of Nuclear Security Culture

Important: The anonymity of this survey will be protected, no names will be used and its results will be utilized exclusively for the evaluation of nuclear security culture at this organization. The only information requested from respondents is whether they belong to security or non-security personnel. Please check one box below. This identification will facilitate the process of assessment.

☐ **Security personnel**

☐ **Non-security personnel**

INSTRUCTIONS

First: The purpose of a security culture self-assessment is to support high levels of security performance by providing a clear picture of the influence of the human factor on the organization's security regime. This survey is just the first stage in this process. The results of the self-assessment will be shared with all personnel.

Second: You are requested to evaluate the key characteristics of security culture in this organization by comparing what the culture is to what it should be. The scoring scheme is based on a 7 point scale ranging from 'strongly disagree' (1) to 'strongly agree' (7). The scheme denotes that this particular indicator is either fully observed and present, completely unobserved and absent, or partially present and visible. Please check 'neither agree nor disagree' if you do not have any opinion regarding the statement and briefly explain why in the comments box. Check the 'non-applicable' or N/A box if you have insufficient or no information whatsoever regarding the issue raised in the statement.

Third: If you would like to provide additional information, please leave your comments in the space at the bottom of the page and identify the statements to which they belong. Your comments will be an important contribution to the self-assessment process.

Fourth: The survey is anonymous. You do not have to identify yourself or to sign the survey form. When you complete the survey, fold it and drop it in the box with the sign 'Survey: Security Culture Self-Assessment' located in ___ [indicate its location].

Fifth: If you have any questions after completion of the survey please contact the Self-Assessment Team listed below.

[List names of self-assessment team members.]

FIG. 9. Survey instructions.

Strongly disagree	Disagree	Somewhat disagree	Neither Agree Nor Disagree (Explain Why)	Somewhat agree	Agree	Strongly agree
1	2	3	4	5	6	7
(1) I am aware of the nuclear security policy at my organization to the extent that I can specifically cite its provisions relevant to my job.						
Please write any other comments at the bottom of the page.						

FIG. 10. Example of survey question and answer space.

Appendix VI

INTERVIEW

VI.1. Interviews have the following advantages as a self-assessment method:

— They are useful for gaining insights, perceptions and overall context.
— They allow interviewees to focus on what is important to them.
— They can provide new perspectives on a topic.
— They enable the clarification of some ambiguities identified by other assessment methods.

However, their limitations must also be considered:

— They are time consuming and labour intensive compared with other data collection methods.
— They are susceptible to interviewers' bias.
— They require training for interviewers.
— They may seem intrusive to interviewees.

Semistructured interviews can be used in the culture self-assessment process to ascertain qualitative data that surveys do not reveal — such as past experiences, inner perceptions and attitudes and feelings about reality — by giving respondents the time and freedom to discuss particular topics. The objective of these interviews is to understand the respondent's point of view rather than to make generalizations about any particular topic.

VI.2. The breadth and the depth of the self-assessment team's professional experience, including its interviewing and analytical skills, will determine the extent to which semistructured interviews can be used effectively as a tool of self-assessment. Specifically, if the team has relatively junior individuals who may not fully understand how different security and non-security functions and processes are carried out within the organization, management should reinforce the team by assigning better informed and more experienced individuals from different departments and levels, ensuring full coverage and integration.

STEP 1: INTERVIEW GUIDE

VI.3. It is important for the interviewers to prepare an interview guide on the basis of surveys or other analyses that yield groupings of themes and questions

to be posed to interviewees in different contexts. The interview guide should be shared with all interviewers. Qualitative data relevant to the self-assessment may be derived from carefully managed discussions of:

(a) How the organization decides what is correct and important;
(b) Why decision making patterns flow the way they do;
(c) What people take for granted in their reasoning about security;
(d) How the dynamics within the organization determine what the leadership pays attention to and what it ignores.

VI.4. Therefore, the development of the interview guide should take into consideration the self-assessment's focus, the specific information interviewers want to learn from persons they plan to speak with, how much the self-assessment team already knows about the question, and logistical issues such as the amount of time allocated for each session.

VI.5. Ideally, interview guides are continually evolving tools. Questions are developed, tested and then refined based on what is learned from asking them. To this end, members of the team share the results of each interview with one another prior to any subsequent interview in order to:

(a) Look at what kind of discussion emerges when certain questions are asked and find out which questions need to be refined;
(b) Find a way to separate individual views and perceptions relevant to self-assessment from comments that interviewees believe would please the team and the management;
(c) Identify new experiences shared by team members that might be investigated further in subsequent sessions;
(d) Identify further potential interviewees based on the recommendations of interviewees who have already participated;
(e) Reflect on the interviewer's role, preconceptions and behaviours during interviews in order to make necessary adjustments and avoid mistakes.

VI.6. In the preparation stage, it is useful to test the interview guide by conducting a series of informal interviews. Informal interviews foster low pressure interaction and allow respondents to see the interview simply as a conversation, and thus to speak more freely and openly. Informal interviewing may be used to uncover new topics of interest that may have been overlooked by survey analysis and provide a foundation for developing and conducting more structured interviews.

STEP 2: SELECTION OF INTERVIEWEES

VI.7. Compared with the number of survey respondents, interviewees constitute a smaller group. In determining the group's size and composition, the following criteria are taken into consideration:

(a) Those interviewed should be knowledgeable about the focus of the self-assessment and willing to talk about the subject.
(b) As the optimal number of interviewees is typically 5–10% of the target population, the inclusion of diverse professional and demographic groups is very important.
(c) Selected interviewees should include not just those in security and non-security fields, but also administrative staff, the managers of contractors and others with expertise relevant to self-assessment.

VI.8. Professional and personal relationships should be considered. Interviewer and interviewee should not be in the same chain of command, nor should they be relatives or friends. A relaxed atmosphere and absence of superiors are conducive to a free flow of information.

VI.9. An explanatory checklist should be designed to make clear for interviewees:

(a) The purpose of the interview;
(b) The topic under discussion;
(c) The format of the interview;
(d) The approximate length of the interview;
(e) An assurance of confidentiality;
(f) The respondent's right to ask for clarification or to decline to comment;
(g) The purpose of audio or video recordings (which may only be made with explicit permission).

VI.10. Taking the time to explain how the interview will work can be very helpful in ensuring a smooth and fruitful interview. Ultimately, it will be for the interviewer to decide the best way to do this according to the cultural context. The interviewer should assume that there are no right or wrong answers; it is personal opinions and perspectives that are of interest to the self-assessment. It is also important to emphasize the voluntary nature of the interview.

STEP 3: CONDUCT OF INTERVIEWS

VI.11. Interviews should be conducted in a private location with no outsiders present and where people feel their confidentiality is protected. In the initial stage of the interview, interviewees often exhibit signs of uneasiness and uncertainty. Therefore, starting with some general conversation can help respondents to relax. Rapport with the interviewee is critical to eliciting candid and valid information. Explaining the benefits of understanding culture helps to motivate interviewees, as does discussing how information obtained during the interview can help to improve security, safety and organizational effectiveness. After an introductory general question based on the topic under discussion (e.g. "What is your personal role in and contribution to maintaining and improving nuclear security in the organization?"), it is useful to ask 'prompt' questions that help to identify key issues while guiding the interview along the desired path.

VI.12. Prompt questions ask interviewees to describe something familiar that is also central to the self-assessment topic (e.g. specific examples of past or current practices). These questions are crucial for the interview process because they help establish a framework for discussion and draw out initial information, especially if interviewees provide few details on their own. Prompt questions create a setting for open ended questioning — the main rationale behind interviews — and deepen the inquiry by encouraging participants to consider and reveal their true feelings. Prompt questions should, however, be phrased carefully to avoid steering the interviewee towards predetermined conclusions.

VI.13. Open ended questions are formulated on the basis of survey analysis and can paraphrase indicators that were not used in the survey. Open ended questions set no limit on the scope or length of responses, instead giving interviewees the opportunity to explain their position, feelings or experiences. An example is: "Would you please describe the ranking of nuclear security in the overall priority list of the organization?"

VI.14. To help understand the interviewee's perceptions and experience, 'probing' questions are frequently used during open ended questioning. Probes are neutral questions, phrases, sounds and even gestures that interviewers use to encourage interviewees to elaborate on their answers and explain relevant circumstances. Suggestions for probes can be outlined in the interview guide, but they are also left to the discretion of the interviewer. Probes are used when interviewees' responses are brief or unclear, when interviewees seem to be waiting for a reaction before continuing to speak or when the interviewee appears to have more information on the subject being discussed. Excessive probing may

be counterproductive. If responses are repetitive or lacking in substance, or if the interviewee becomes irritated or upset about questions on a particular topic, it is best to advance to the next question.

VI.15. Probing is possibly the most important technique in interviewing, but it is also the hardest to master. It requires practice, thorough knowledge of the assessment objectives and the interview guide as well as a solid understanding of what kind of information each question is intended to elicit. It also requires patience and sensitivity, effective time management and good interpersonal skills. Probing techniques include echoing, whereby the interviewer repeats the point expressed by the interviewee to encourage him or her to develop it further; verbal agreement, whereby the interviewer expresses interest in the interviewee's views through brief phrases indicating concurrence; the 'tell me more' approach, whereby the interviewer explicitly asks the interviewee to expand on a particular point; and culturally appropriate body language such as nodding in acknowledgement.

VI.16. It is important to avoid common interviewing errors:

(a) Asking leading questions or giving leading examples in an effort to make the question clearer:
   — Examples offered tend to direct respondents in a direction they might not have gone without an example.
   — Questions should be crafted to ensure clarity, and clarification should be given by rephrasing the question rather than supplying an example.

(b) Rushing into pauses during the interviewee's answer:
   — When there is a gap in the conversation, many interviewers are tempted to immediately ask another question or provide a summary that puts words into the interviewee's mouth.
   — Attentiveness and body language, along with silence, encourage the interviewee to say more or go into an answer more fully, often providing deeper information about culture.

(c) Underestimating the significance of non-verbal communication:
   — How the interviewer communicates non-verbally has a significant impact on the interviewee.
   — Techniques such as maintaining eye contact, leaning forward and using encouraging facial expressions, where culturally appropriate, can reinforce the impression of interest and attention, and promote conversation.

STEP 4: NOTE TAKING AND RECORDING

VI.17. Since semistructured interviews contain open ended questions and discussions may diverge from the interview guide, it is generally best to record the interviews and, if circumstances permit, transcribe them for analysis. Making written notes of answers while also trying to conduct an interview is likely to result in both poor notes and in a weaker rapport between interviewer and interviewee. Development of rapport and dialogue is essential in semistructured interviews. If a respondent does not agree to recording the interview, a notetaker should be present.

VI.18. Deciding when to end an interview is at the interviewer's discretion, but is generally done when the topic has been covered comprehensively, no new information appears likely to emerge or the interviewee seems tired or has other commitments to attend to. A good practice is for the interviewer to summarize the key points provided during the session, giving the respondent a final chance to expand upon, clarify or correct any point.

VI.19. It is important to have a good data collection and management process in order to store, retrieve and analyse the data from interviews for the present and any future self-assessments. Once the highlights of all the interviews have been transcribed or the notes written up, the self-assessment team should review the transcripts or notes. Doing so may give rise to a fresh perspective, filling in gaps, providing new clues, confirming or contradicting initial assumptions, and facilitating interpretation of the data.

CONTINUOUS SKILLS IMPROVEMENT

VI.20. The interviewer's skills have an important influence on the usefulness of the information that interviewees provide. The interviewer should be able to be sympathetic without counselling, to encourage interviewees to elaborate on their answers without expressing approval, disapproval, judgement or bias, and to keep track of the questions while letting the conversation develop naturally. The core skills needed to establish positive rapport between interviewer and interviewee are emphasizing the interviewee's perspective and accommodating different personalities and emotional states. The key skills for effective interviewing are described in Table 3.

TABLE 3. KEY SKILLS FOR EFFECTIVE INTERVIEWING

Skills	Description
Rapport building	The ability to quickly create interviewer–interviewee dynamics that are positive, relaxed and mutually respectful
Emphasizing the interviewee's perspective	Treating the interviewee as an expert, balancing deference to the interviewee with control over the interview, being an engaged listener, demonstrating a neutral attitude
Adapting to different personalities and emotional states	Being able to quickly adjust interviewing style to suit each individual interviewee

Appendix VII

DOCUMENT REVIEW

VII.1. Document review has the following advantages as a self-assessment method:

— It is a good source of background information.
— It may identify security related issues not clearly identified by other means.
— It is unobtrusive and relatively inexpensive.
— It can provide relevant information from different time periods enabling the study of trends.
— Few biases can be expected in the collected data.
— Information in documents is independently verifiable.

However, its limitations must also be considered:

— It can be time consuming to collect, review and analyse many documents.
— The confidential nature of some documents may prevent their use in a widely circulated final report.
— It may be representative of only one perspective on the issue under consideration.

Use of document review throughout all steps of the self-assessment serves a useful purpose only if the self-assessment team is fully aware of its advantages and limitations. The purposes of conducting a document review are as follows:

(a) To collect background information as a general context for self-assessment. Reviewing past and present documents helps the reviewer to understand the history, philosophy and operation of the nuclear security culture in a given organization.
(b) To compare actual implementation with decisions and intention in reviewed documents. The review of documents may reveal a difference between formal statements and intentions on one side and their actual implementation on the other. It is important to determine if such a difference exists and identify possible reasons for such gaps through other means.
(c) To validate results obtained from other sources and facilitate self-assessment analysis. The self-assessment team can double check information generated by other self-assessment tools and, if needed, facilitate preparation for surveys, interviews and observations.

(d) To acquire factual data about the issues under review. Reviewing documents is useful to create a comprehensive picture by adding, for example, the number and type of participants in security relevant events or the sequence of training sessions.

VII.2. The following practical steps are suggested for conducting a document review:

(1) Assess existing documents. Find out what types of documents exist and determine which of them can clarify specific issues.
(2) Secure access to the documents identified as relevant to the self-assessment. Certain documents may only be accessed with the permission of others, or are of a confidential nature. Often, senior management and legal experts need to provide authorization for access to them.
(3) Ensure confidentiality regarding the use of any documents not in the public domain. Confidentiality is always an important consideration when collecting data for self-assessment. Development of appropriate guidelines can help secure access to sensitive and confidential documents.
(4) Compile the documents relevant to the self-assessment. Once access to the documents relevant to the self-assessment has been secured, they need to be compiled, but the review should be focused on the self-assessment only.
(5) Develop a document review protocol, checklist or examination form. These should be systematically used by each reviewer to ensure that the necessary information is identified, analysed, codified and documented. Each protocol, checklist or form should include space at the top to discuss the document and where it is stored if additional information is needed later. It is useful to provide a positive example of a completed review protocol, checklist or examination form, highlighting how information can be recorded on the form to maximize its clarity and usability.
(6) Determine the accuracy of the documents. This may involve comparing documents that contain similar information, checking the documents against other collected data and speaking with people who were involved in the development of the document.
(7) Convene a reviewer brainstorming session. When all the selected documents have been reviewed, all the reviewers meet to collectively document the findings of their reviews. In particular, the reviewers identify specific instances where information from different documents may disagree, instances where numerous documents contain similar information and where additional information might be found, as well as how the findings fit into the self-assessment mission.

(8) Summarize the information from the document review. A report on the results of the document review and preliminary conclusions is shared with the entire self-assessment team as an input to the self-assessment process.

Appendix VIII

OBSERVATION

VIII.1. Observation has the following advantages as a self-assessment method:

— It is possible to directly observe what people do rather than relying on what they say they do.
— It does not rely on people's willingness to provide information.
— It is possible to collect data at the point where and when an event or activity is occurring.

However, its limitations must also be considered:

— Only a limited number of people or events can be observed leading to a danger of generalization based on a small number of cases.
— It is susceptible to observer bias.
— People usually perform better when they are aware of being observed.
— It does not increase the understanding of why people behave the way they do.

Observation is a multistage process which includes the following:

(a) Determination of the observation object or target;
(b) Selection of the method of filing results;
(c) Development of an observation plan;
(d) Selection of data processing methods;
(e) Conduct of observations;
(f) Interpretation of accumulated data and consolidation with other self-assessment results.

VIII.2. In the process of observation the focus is on:

(a) The physical setting;
(b) The activities observed;
(c) The human social environment (the way in which human beings interact, patterns of interactions, frequency of interactions, direction of communication patterns, decision making patterns);
(d) Formal interactions;
(e) Informal interactions and improvised activities;
(f) Non-verbal communication.

VIII.3. Observations typically incorporate a prescribed protocol containing specific measures of observable behaviour. Three types of data can be gathered from observations: descriptive information, where the assessor notes what was actually seen (e.g. a security portal closed for maintenance during the morning peak hours with employees arriving to work and walking through another gate without inspection); inferred information, whereby the observer makes inferences about underlying dynamics (e.g. a security officer who requires contractors to remove their coats before passing through security controls, but allows staff members to enter without removing theirs); and evaluative observations, where the assessor both infers from and judges the behaviour witnessed. (E.g. the assessor wants to investigate whether pre-task briefings are routinely used to enhance compliance with security related procedures. This observation assumes that pre-task briefings are useful for preventing security breaches and that those who undergo briefings easily internalize the information provided. Such assumptions can be later validated only through interviews.)

VIII.4. Observational information comes mainly from observational notes. Effective use of observation depends on the ability to develop notes as well as to analyse and store them. Following each observation event, data collectors need to expand their notes into rich descriptions of what they have observed. This involves transforming raw notes into a narrative and elaborating on initial observations. It is important to minimize the time between the observation and the writing of the field notes.

VIII.5. Expanding observational notes involves the following:

(a) Scheduling time to expand notes, preferably within 24 hours from the time field notes are made. Good note taking often triggers the memory, but with the passage of time, this opportunity is lost.
(b) Expanding shorthand notes into sentences so that other members of the team can read and understand. Depending on circumstances, it would be useful to expand and type the notes into a computer file shared with the self-assessment team.
(c) Composing a descriptive narrative from shorthand, observations and key words. A good technique for expanding notes is to write a narrative of what occurred and how this event can be interpreted. The narrative may be the actual document to be used in the self-assessment process. Its text should have clearly labelled sections to report objective observations and interpretation and personal comments.

VIII.6. The observational notes should include as a minimum the following:

(a) Location and duration of the observation;
(b) List of involved staff with short descriptions of responsibilities;
(c) List of topics (in observed meetings and discussions);
(d) Observed behavioural patterns, especially when related to security;
(e) A general estimate of people's interaction related to security.

VIII.7. Arrangements can be made with the management to archive observational notes and store them for a specified amount of time. The value of observational notes goes beyond security.

Appendix IX

SECURITY MANAGEMENT SYSTEM INDEXES FOR CONDUCTING OBSERVATIONS

IX.1. The objective of Table 4 is to provide select fact based indexes that help the management to conduct observations regarding the completeness of the security management systems and their ability to function as required. They are to be periodically used by managers to identify deficiencies and gaps in the systems and thus diagnose not only their status but also possible implications for personnel behaviour.

IX.2. These indexes can send an early signal to justify a self-assessment or contribute to its process by providing additional factual inputs to cultural (behavioural) assessments.

TABLE 4. SECURITY MANAGEMENT SYSTEM INDEXES

	Index	Remarks
(a)	*Visible security policy*	
(1)	A nuclear security policy has been established for the organization and is posted in facilities and offices	
(2)	A staff code of conduct exists, which covers the needs of nuclear security	
(3)	Ongoing training and awareness sessions include the code of conduct	
(4)	Management provides resources for security as planned	
(5)	Processes are in place to identify the mandatory requirements relating to security	
(6)	Nuclear security policy is kept up to date	
(7)	Regularly held management meetings in the organization cover significant security items	

TABLE 4. SECURITY MANAGEMENT SYSTEM INDEXES (cont.)

	Index	Remarks
(8)	Events related to the threat environment and its potential impact on nuclear security and nuclear security policy are reported to all staff	
(9)	Professional rewards or recognition is associated with the achievement of nuclear security policy goals	
(10)	Media based communication systems (Intranet, newsletters, and the like) are used to disseminate the security policy to staff members and contractors	
(b)	*Clear roles and responsibilities*	
(1)	Roles and responsibilities for all nuclear security positions are clearly defined in relevant documents	
(2)	Initial briefings and/or training sessions cover security roles and responsibilities	
(3)	Responsibility for security is assigned to a senior member of the management team	
(4)	Security processes and procedures are clearly defined in relevant documents	
(5)	Contractual documents clearly define contractors' roles and responsibilities in nuclear security	
(6)	The threat against which nuclear and radioactive material should be protected (e.g. the DBT) has been determined and made known to relevant parties involved in designing, applying and evaluating the security measures	
(c)	*Performance measurements*	
(1)	The organization uses benchmarks and targets in order to understand, achieve and improve performance at all levels	
(2)	Performance results compared with the targets are regularly communicated to the staff	
(3)	Action is taken when nuclear security performance does not fully match goals	

TABLE 4. SECURITY MANAGEMENT SYSTEM INDEXES (cont.)

	Index	Remarks
(4)	Effective performance leading to better security is rewarded	
(5)	Regulatory and independent self-assessments of security performance are performed and discussed at management and other meetings	
(6)	The organization actively and systematically monitors performance	
(d)	*Work environment*	
(1)	Staff are consulted about the ergonomics and effectiveness of their work environment	
(2)	Top managers periodically visit manned security posts	
(3)	Written procedures exist for all significant security activities	
(4)	Feedback from staff members and contractors is requested and analysed	
(5)	Overtime to prevent adverse security implications is monitored and controlled	
(6)	Procedures are regularly reviewed and updated	
(e)	*Training and qualifications*	
(1)	A comprehensive nuclear security training programme exists, with requirements and qualification standards established, documented and communicated to personnel	
(2)	Periodic evaluation of security training programmes is conducted and revisions incorporated	
(3)	Physical fitness criteria for guards are established and monitored	
(4)	Basic security awareness training instructs all staff on proper workplace security including requirements for reporting security violations	

TABLE 4. SECURITY MANAGEMENT SYSTEM INDEXES (cont.)

	Index	Remarks
(5)	A performance testing programme is in place to ensure procedures and practices learned in training are applied in practice	
(6)	Leadership skills and good practice in security are included in training programmes for managers and supervisors	
(7)	Management provides resources for effective training	
(8)	Security and non-security employees participate in refresher training to improve security related knowledge and skills	
(9)	Beliefs and attitudes are considered in security training	
(10)	Management participates in nuclear security training	
(11)	Training materials include good practices and lessons learned from security events	
(12)	The absentee rate during training sessions on nuclear security is low	
(13)	Staff are trained on performance testing	
(f)	*Work management*	
(1)	A work plan for maintaining the integrity of the nuclear security system exists	
(2)	Contingency plans are established to address foreseeable events	
(3)	Security policy is reviewed regularly and updated if necessary	
(4)	There are written policies, rules and procedures for recruitment, appraisal and termination of employment as they pertain to security	
(g)	*Information security*	
(1)	Classification of documents and control requirements are defined and documented	

TABLE 4. SECURITY MANAGEMENT SYSTEM INDEXES (cont.)

	Index	Remarks
(2)	Processes and protocols exist for classifying and handling information	
(3)	Classified information is securely segregated, stored and managed	
(4)	Employees are given training on the importance of adhering to the requirements of information protection	
(5)	The requirements and procedures for security of computer based systems are defined and documented	
(6)	Access to information assets is restricted to those who need such access and have been subjected to a trustworthiness check	
(7)	An information and computer security function is established, funded and staffed	
(8)	Documented IT security policy covering all information carriers exists	
(9)	Processes and protocols for operating computer systems have been compiled both inside and outside the organization	
(h)	*Operations and maintenance of security systems*	
(1)	Operation and maintenance are performed according to approved procedures and vendor schedules	
(2)	Checklists and detailed procedures for operation and maintenance exist	
(3)	Requirements and procedures for compensation availability of security equipment are planned and documented	
(4)	Operational experience including false and nuisance alarm rates is recorded and analysed for maintenance and in planning purchases	
(5)	Operations and maintenance procedures have been established	
(6)	Procedures for work orders for repair and maintenance of security equipment and hardware exist	

TABLE 4. SECURITY MANAGEMENT SYSTEM INDEXES (cont.)

	Index	Remarks
(7)	Maintenance is performed on schedule	
(8)	There is a system for documenting historical data on equipment and maintenance actions	
(9)	There are procedures in place defining and controlling maximum times for repairing security equipment	
(10)	Critical spare parts and tools are available when needed	
(11)	Workplace forums are convened regularly for discussing issues of mutual interest to operations and maintenance staff	
(12)	The organization has a calibration plan for security equipment such as radiation detectors, metal detectors and other security devices requiring calibration	
(i)	*Determination of staff trustworthiness*	
(1)	Documented staff and contractor screening processes are matched using a graded approach to the access requirements associated with the specific employment roles and responsibilities	
(2)	The trustworthiness programme includes risk factors such as mental illness, drug and alcohol abuse	
(3)	Screening processes are required for and applied to all levels of the organization, including temporary staff and contractor personnel and visitors	
(4)	Real or apparent failures of the screening processes are appropriately investigated and adjudicated	
(5)	The importance of trustworthiness is included in staff training	
(6)	Training is provided to management and other appropriate personnel to guide them in identifying apparent high risk behavioural symptoms	
(7)	An insider threat mitigation programme is in place	

TABLE 4. SECURITY MANAGEMENT SYSTEM INDEXES (cont.)

	Index	Remarks
(8)	The staff trustworthiness determination is periodically reviewed and updated	
(j)	*Quality assurance*	
(1)	Assessment processes are in place for the security function	
(2)	Security processes are prepared, documented, and maintained in accordance with recommended quality assurance standards (recording of formal approval, periodic and planned review, testing, lessons learned, etc.)	
(3)	Quality assurance measures are enforced	
(4)	Quality assurance procedures are periodically evaluated against good practices for the industry	
(k)	*Change management*	
(1)	Change management processes are in place for changes that could affect the security function	
(2)	Changes in such areas as operations, safety and security are coordinated with all potentially affected organizations	
(3)	Assessments are made of changes to confirm that the desired outcomes have been obtained	
(4)	All staff members and contractors who are affected by changes receive the necessary training to handle the change	
(5)	Responsibilities and accountabilities for carrying out security related work are defined and documented in the context of change management	
(6)	Baseline standards in procedures and facility design are established and changes from baseline are documented	
(7)	Before modifying or acquiring hardware, software and equipment, task analyses are performed that take human factors into consideration	

TABLE 4. SECURITY MANAGEMENT SYSTEM INDEXES (cont.)

	Index	Remarks
(8)	Before implementing changes to procedures, equipment or organizational structure a communication process is established for staff members and contractors	
(l)	*Feedback process*	
(1)	Processes are in place to obtain, review and apply available national and international information that relates to the security function and the nuclear security system	
(2)	Processes are in place to allow and encourage members of the public, staff and contractors to report abnormal conditions to the management	
(3)	Reports related to security are reviewed by management with actions taken	
(4)	Documented and established review systems for processes and procedures are in place to solicit comments and inputs from relevant employees and contractors within the organization	
(5)	Discussion of pending security related issues and changes are encouraged	
(m)	*Contingency plans and drills*	
(1)	Contingency plans are in place and are periodically exercised	
(2)	All security systems are tested periodically including systems that are not activated during normal operation	
(3)	Contingency plans are coordinated with and linked to a relevant national strategy	
(4)	Contingency plans are tested and coordinated with off-site backup forces	
(5)	Managers are trained to deal with novel or exceptional situations	
(6)	Provisions are in place to ensure that security can be adjusted in response to increased threat	

TABLE 4. SECURITY MANAGEMENT SYSTEM INDEXES (cont.)

	Index	Remarks
(7)	The organization provides relevant information on potential risks to public authorities such as first responders, the police, the military, medical facilities and environmental authorities	
(n)	*Self-assessment*	
(1)	A documented self-assessment programme defining self-assessment processes is in place	
(2)	Deficiencies are analysed to identify and correct emerging trends	
(3)	Performance is benchmarked to compare operations against national and international good practices	
(4)	Operational performance is observed and evaluated	
(5)	Corrective action plans are developed on the basis of self-assessment findings and implementation of these plans is tracked	
(6)	There is an established procedure to continuously monitor security culture through use of indicators to implement improvements and prevent the degradation of security culture	
(7)	Self-assessment results are shared to the extent possible throughout the industry as part of the exchange of good practices	
(o)	*Interface with the regulator (and law enforcement bodies)*	
(1)	Information is regularly exchanged between the regulatory body and the organization	
(2)	Information regarding vulnerabilities and threats is mutually relayed	
(3)	Regulatory interface roles are clearly defined and interagency processes are streamlined	
(4)	The regulatory body's responsibility is explained in training programme	

TABLE 4. SECURITY MANAGEMENT SYSTEM INDEXES (cont.)

	Index	Remarks
(p)	*Coordination with off-site organizations*	
(1)	Staff and management level communication with local and national organizations involved in nuclear security occurs regularly	
(2)	Written agreements on assistance, communication and timely response to incidents are in place with appropriate organizations	
(3)	There are memoranda of understanding for performing off-site and on-site security exercises	
(4)	The organization conducts a response assessment exercise	
(5)	Contractors are trained on security procedures prior to starting work	
(6)	Outside stakeholders are involved when problems are being solved and decisions are being made	
(7)	Communication and cooperation with current and potential suppliers and contractors cover security related issues	
(8)	Participation in external security related courses and events is encouraged and supported by management	
(9)	International publications and reports covering nuclear security are available to staff	
(10)	The organization is open to international cooperation on nuclear security issues, including research and technical exchange visits	
(11)	Nuclear security information from international publications is made available to staff	
(q)	*Record keeping*	
(1)	A record keeping system for security programme related information exists	
(2)	Records and log books are accessible to those who need them for the performance of their duties	

TABLE 4. SECURITY MANAGEMENT SYSTEM INDEXES (cont.)

	Index	Remarks
(3)	A requirement for the regular analysis of records exists	
(4)	There is a policy for protection of confidential records	

REFERENCES

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

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

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

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

[5] 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 CRIME, 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).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8, IAEA, Vienna (2008).

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

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Sources, IAEA Nuclear Security Series No. 11, IAEA, Vienna (2009).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme, IAEA Nuclear Security Series No. 19, IAEA, Vienna (2013).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, IAEA, Vienna (2011).

[11] Amendment to the Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1/Mod.1, IAEA, Vienna (2016).

[12] Code of Conduct on the Safety and Security of Radioactive Sources, IAEA/CODEOC/2004, Vienna (2004).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, OSART Independent Safety Culture Assessment (ISCA) Guidelines, IAEA Services Series No. 32, IAEA, Vienna (2016).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Performing Safety Culture Self-assessments, Safety Reports Series No. 83, IAEA, Vienna (2016).

[15] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Key Practical Issues in Strengthening Safety Culture, INSAG-15, IAEA, Vienna (2002).

[16] SCHEIN, E., Organizational Culture and Leadership, 4th edn, Jossey-Bass, San Francisco, CA (2010).
[17] SCHEIN, E., The Corporate Culture: Survival Guide, Jossey-Bass, San Francisco, CA (1999).

GLOSSARY

contingency plan. Predefined sets of actions for response to unauthorized acts indicative of attempted unauthorized removal or sabotage, including threats thereof, designed to effectively counter such acts.

human factor. The complex of all individual and collective human physical, psychological and behavioural properties that interact with technological systems, management organizations and the natural environment.

indicator. A security culture characteristic that can be observed or measured to compare with criteria as a means of assessing the strength of the nuclear security culture.

insider. An individual with authorized access to associated facilities or associated activities or to sensitive information or sensitive information assets, who could commit or facilitate the commission of 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.

nuclear security culture. The assembly of characteristics, attitudes and behaviour of individuals, organizations and institutions that serves as a means to support, enhance and sustain nuclear security.

IAEA
International Atomic Energy Agency

No. 25

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.

CANADA

Renouf Publishing Co. Ltd
22-1010 Polytek Street, Ottawa, ON K1J 9J1, CANADA
Telephone: +1 613 745 2665 • Fax: +1 643 745 7660
Email: order@renoufbooks.com • Web site: www.renoufbooks.com

Bernan / Rowman & Littlefield
15200 NBN Way, Blue Ridge Summit, PA 17214, USA
Tel: +1 800 462 6420 • Fax: +1 800 338 4550
Email: orders@rowman.com Web site: www.rowman.com/bernan

CZECH REPUBLIC

Suweco CZ, s.r.o.
Sestupná 153/11, 162 00 Prague 6, CZECH REPUBLIC
Telephone: +420 242 459 205 • Fax: +420 284 821 646
Email: nakup@suweco.cz • Web site: www.suweco.cz

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: formedit@formedit.fr • Web site: www.form-edit.com

GERMANY

Goethe Buchhandlung Teubig GmbH
Schweitzer Fachinformationen
Willstätterstrasse 15, 40549 Düsseldorf, GERMANY
Telephone: +49 (0) 211 49 874 015 • Fax: +49 (0) 211 49 874 28
Email: kundenbetreuung.goethe@schweitzer-online.de • Web site: www.goethebuch.de

INDIA

Allied Publishers
1st Floor, Dubash House, 15, J.N. Heredi Marg, Ballard Estate, Mumbai 400001, INDIA
Telephone: +91 22 4212 6930/31/69 • Fax: +91 22 2261 7928
Email: alliedpl@vsnl.com • Web site: www.alliedpublishers.com

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

JAPAN

Maruzen-Yushodo Co., Ltd
10-10 Yotsuyasakamachi, Shinjuku-ku, Tokyo 160-0002, JAPAN
Telephone: +81 3 4335 9312 • Fax: +81 3 4335 9364
Email: bookimport@maruzen.co.jp • Web site: www.maruzen.co.jp

RUSSIAN FEDERATION

Scientific and Engineering Centre for Nuclear and Radiation Safety
107140, Moscow, Malaya Krasnoselskaya st. 2/8, bld. 5, RUSSIAN FEDERATION
Telephone: +7 499 264 00 03 • Fax: +7 499 264 28 59
Email: secnrs@secnrs.ru • Web site: www.secnrs.ru

UNITED STATES OF AMERICA

Bernan / Rowman & Littlefield
15200 NBN Way, Blue Ridge Summit, PA 17214, USA
Tel: +1 800 462 6420 • Fax: +1 800 338 4550
Email: orders@rowman.com • Web site: www.rowman.com/bernan

Renouf Publishing Co. Ltd
812 Proctor Avenue, Ogdensburg, NY 13669-2205, USA
Telephone: +1 888 551 7470 • Fax: +1 888 551 7471
Email: orders@renoufbooks.com • Web site: www.renoufbooks.com

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

Marketing and Sales Unit
International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 or 22530 • Fax: +43 1 2600 29302 or +43 1 26007 22529
Email: sales.publications@iaea.org • Web site: www.iaea.org/books

This publication will assist organizations operating facilities and activities that use nuclear and other radioactive material in conducting self-assessments of nuclear security culture by providing practical methods and tools for their conducts. It will also help regulatory bodies and other competent authorities to understand the self-assessment methodology used by operators to encourage operators to start the self-assessment process or, if appropriate, to conduct independent assessments of nuclear security culture. This publication is the first practical guidance on the concept of nuclear security culture since the issuing of IAEA Nuclear Security Series No. 7, Nuclear Security Culture, in 2008.

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 978–92–0–111616–1
ISSN 1816–9317