IAEA SECURITY SERIES NO. XX

NST026

DRAFT, 2 July 2014

STEP 8: Submission to Member States for comment

SELF-ASSESSMENT OF NUCLEAR SECURITY CULTURE IN FACILITIES AND ACTIVITIES THAT USE NUCLEAR AND/OR RADIOACTIVE MATERIAL

DRAFT TECHNICAL GUIDANCE

INTERNATIONAL ATOMIC ENERGY AGENCY

VIENNA, 20XX

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 in 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 country, 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 Agency'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 world-wide.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

An effective nuclear security culture depends on proper planning, training, awareness, operations and maintenance, as well as on the thoughts and actions of people who plan, operate and maintain nuclear security systems. An organization may be technically competent while remaining vulnerable if it discounts the role of the human factor. Thus the human factor (including the upper tier of managers and leaders) is important to effective nuclear security.

In 2008, the IAEA published an Implementing Guide on nuclear security culture in its Nuclear Security Series [1]. The Implementing Guide defines the concept and characteristics of nuclear security culture while describing the roles and responsibilities of institutions and individuals entrusted with a function in the security regime. Since then, the IAEA has conducted many international, regional, and national workshops to promote security culture and train nuclear industry personnel at all levels.

The IAEA has developed a comprehensive methodology for evaluating security culture which is being promoted for practical use. Such a methodology will help make security culture sustainable. It will also promote cooperation and the sharing of best practices related to nuclear security culture.

A self-assessment methodology, complete with indicators for assessment, will assist Member States in determining how best to strengthen their nuclear security culture. This publication is the first guidance for assessing nuclear security culture and analysing its strengths and weaknesses in a nuclear facility or organization. It reflects, within the context of assessment, the nuclear security culture model, principles and criteria set down in the Implementing Guide.

Devising a methodology poses a challenge, however, since culture is composed of intangible human characteristics such as beliefs, attitudes, values and ethics. Fostering it demands a multidisciplinary approach. Unlike traditional performance audits, security culture self-assessment can help an organization benefit from an important learning curve. This applies not only to security professionals, but also to the entire personnel. Such introspection provides an opportunity for the organization to grasp how culture influences security performance. Self-assessment encourages staff members to take ownership of the results, and it facilitates decisions that foster continued learning and improvement.

1.2. OBJECTIVE

This publication is intended for use by senior managers and security specialists in organizations operating nuclear facilities to assist them in assessing the nuclear security culture in their organization as a basis for identifying ways to strengthen that culture. This guidance might also be useful for

regulatory bodies or other competent authorities to understand the self-assessment methodology used by the operator, to encourage the operator to start the self-assessment process or, if appropriate, to conduct an independent assessment.

1.3. SCOPE

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

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

1.4. STRUCTURE

Following this Introduction, Section 2 describes the IAEA concept and the model of nuclear security culture as an essential element of a nuclear security regime. Section 3 underscores the need to assess 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 with any other culture—by employing certain indicators and indexes. 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 must be interpreted in detail to comprehend what is driving the staff's behaviour in security-related situations and identify measures to boost future performance. Section 7 covers the final stage of the self-assessment process when the report is assembled and shared with the organization, including devising a follow-up action plan to enhance the culture. Nine appendixes (I–IX) provide additional guidance about the IAEA nuclear security culture concept, indicators, the preparation of surveys, graphic 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

2.1. IAEA MODEL OF NUCLEAR SECURITY CULTURE

Essential Element 12 of the Nuclear Security Fundamentals [2] includes "Developing, fostering and maintaining a robust nuclear security culture". Nuclear security culture is defined as "the assembly of characteristics, attitudes and behaviour of individuals, organizations and institutions which serves as a means to support and enhance nuclear security." [1] The role of culture can be deduced from the Agency's 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] Developed in the aftermath of the 9/11 terrorist acts, this updated concept of nuclear security is noteworthy in that it goes beyond traditional material and bureaucratic measures such as physical protection, accounting, and control. This cross-cutting concept—explicitly or implicitly—covers a much wider field. Accordingly, nuclear security culture and its assessment methodology must be universal and apply to all types of nuclear facilities and activities. Figure 1 represents the IAEA Model of nuclear security culture set forth in the 2008 Implementing Guide.

Figure 1. IAEA Model of nuclear security culture.

The IAEA Nuclear Security Plan for 2014–2017 [3] reaffirms that a sustainable nuclear security culture is needed to manage activities involving nuclear and other radioactive materials. Under the framework of the IAEA Plan, implementing sustainable nuclear security in States requires adequate time for the institutionalization of a functioning nuclear security culture. The Plan provides a roadmap for achieving these goals.

The IAEA has conducted numerous international, regional, and national training workshops on nuclear security culture at sites spanning the globe.

Appendix I contains a more detailed description of the IAEA's model of nuclear security culture as well as its theoretical constructs and underpinnings.

2.2. INTERNATIONAL LEGAL INSTRUMENTS

Security culture is one of the 12 Fundamental Principles codified in the 2005 Amendment to the 1980 Convention on Physical Protection of Nuclear Material [4]. Entry into force of the 2005 Amendment would make the Fundamental Principles of nuclear security, including security culture, and binding on States Parties to the Convention.

The term security culture is also found in the 2004 Code of Conduct on the Safety and Security of Radioactive Sources [5]. This Code is non-binding, but over 120 countries have informed the IAEA Director General of their support for it. In addition to international conventions and agreements, numerous IAEA documents in the Nuclear Security Series, known as Fundamentals, Recommendations, Implementing Guides, and Technical Guidance, reiterate the importance of culture for specific elements of nuclear security.

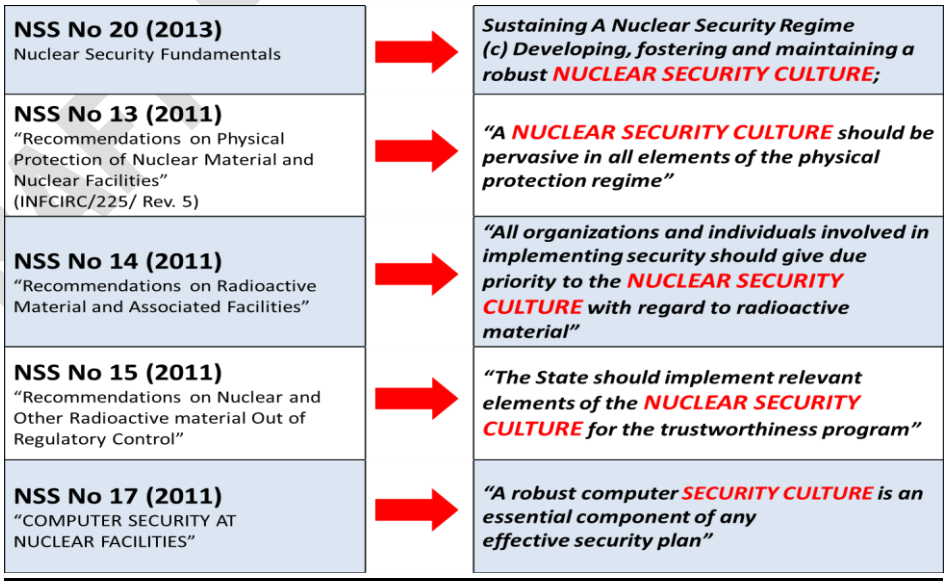

Figure 2. Publications in the IAEA nuclear security series with reference to the application of culture in diverse areas of nuclear security.

3. SELF-ASSESSMENT: CONCEPT AND PRACTICE

3.1. PURPOSE AND BENEFITS OF SECURITY CULTURE SELF-ASSESSMENT

The purpose of a security culture self-assessment is to provide a clear picture of how much nuclear security is part of the organization's culture. This involves evaluating the key characteristics of security culture in the organization by comparing what the culture is at present to their optimal parameters. Such evaluations specify certain indicators as reference level..

Security culture self-assessment plays a key role in developing and maintaining an awareness of the strengths and weaknesses of the organization's nuclear security culture. Due to their heavy focus on perceptions, views and behaviour at all levels of the organization, regular assessments help managers to understand the reasons for an organization's patterns of behaviour in certain circumstances, to devise optimal security arrangements, and to predict how the workforce may react to the unknown. This is in sharp contrast to audit-type assessments, which accentuate technical issues more than intangible human elements. In other words, launching a self-assessment requires 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 actions, but will more typically shed light on why different security-related issues emerge, what the root causes of problems may be, and how security can be enhanced.

Security culture self-assessment helps move the institution along its learning curve, both for those directly involved with security and for the entire organisation, by illuminating how culture influences security performance. An effective self-assessment encourages the staff to accept ownership of the results and facilitates decisions that foster continuous improvement. Examples of specific benefits from self-assessments are:

- Deeper understanding of the human factor and nuclear security culture;
- Clearer understanding of employees' concerns, needs, aspirations, and motives;
- Identification of barriers to and incentives for improvements to security performance;
- Identification of barriers to and motives for change;
- Clarification of employees' opinions about security-related topics;
- Improved capacity to self-assess the organization's security performance, conducting trend analysis within the site or to monitor progress;
- High priority on moves that strengthen the overall organizational culture in areas like internal communication and human resource management.

Assessments of nuclear security culture should complement the currently used methods for evaluating vulnerabilities and nuclear security systems, thus helping the management refine the organization's

overall security arrangements. Practitioners will benefit from an input that is currently missing—the potential of a security-conscious workforce—as they strive to design and maintain adequate security regimes.

3.2. SPECIAL CONSIDERATIONS FOR SECURITY CULTURE SELF-ASSESSMENT

The idea of helping sites self-assess nuclear safety culture had its origins in the 1990s and has made significant progress. The IAEA has released several documents to guide the self-assessment process and share best practices.[1] The agency is finalizing several new documents reflecting the lessons of the 2011 Fukushima accident. It has also been performing safety-culture assessments as part of OSART (Operational Safety and Review Team) missions. In addition, many other organizations, both commercial and non-profit, increasingly provide safety culture assessments. The use of external experts is largely attributed to the lack of in-house expertise in behavioural science, the key to designing assessments and judging their findings.

By releasing this publication on security culture self-assessment, the IAEA is taking initial steps in the same direction. As in the area of nuclear safety, assessment of security culture should ideally include a balance between self-assessment with and without the involvement of outside specialists, as both have their advantages and disadvantages. Self-assessment team members possess in-depth knowledge of the organization, its people, its processes and key influences. They are part of the organization and therefore have a stake in and are more accountable for improvement. On the other hand, however good their intentions, 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 trial stages, and later to verify the self-assessment findings. Such oversight will help managers determine whether the necessary expertise is available internally.

Organizations must be encouraged to develop skills related to self-assessment, including survey protocols, interview techniques, document review, observation methods, and findings analysis. In the light of confidentiality requirements in nuclear security, self-assessment is likely to be the preferred option, but the methodology could also be used for external assessment, including independent assessment by a regulatory body. It is important to bear in mind that the culture of a regulatory body has an impact on the organizational culture of the facility being regulated. The regulator's approach and conduct during such assessment may influence the operating organization's security culture in unintended ways. For this reason a regulatory body conducting independent assessment should be aware of its own security culture and the way it may affect the operator's.

[1] "SCART Guidelines: Reference Report for IAEA Safety Culture Assessment Review Team (SCART)," IAEA Services Series No. 16, 2008; "Safety Culture in Nuclear Installations: Guidance for Use in the Enhancement of Safety Culture," IAEA-TECDOC-1329, 2002; "Self-Assessment of Safety Culture in Nuclear Installations: Highlights and Good Practices," IAEA-TECDOC-1321, 2002; "ASCOT Guidelines: Guidelines for Organizational Self-Assessment of Safety Culture and for Reviews by the Assessment of Safety Culture in Organizations Team," IAEA-TECDOC-743, 1994.

Other distinct features of security culture assessment need to be taken into consideration:

— Subcultures exist within any group, so the overall culture is seldom homogeneous. Cultural analysis should therefore be open to the existence of subcultures and be ready to examine the relationship among them. One important consideration is the difference in perceptions and attitudes between security and non-security personnel. A person who is not part of the facility's security contingent may think security is someone else's responsibility, and that security successes and failures have little to do with anything that person does or fails to do. It is important to view security culture as the sum of these two subcultures, that of security-related positions and that of non-security-related positions. and understanding the differences between security and non-security personnel is vital to a balanced and appropriate assessment.

— While it is safe to assume that most employees take ownership of nuclear safety, security may give rise to divergent views among the workforce. This dichotomy renders the task of self-assessment both challenging and demanding. Below is a sample list of attitudes towards security that security evaluators are likely to encounter over the course of a self-assessment:

  • Ownership (people assume responsibility and regard security as their programme);
  • Participation (people follow the rules while acting like security is not their problem);
  • Apathy (people don't care one way or another about security);
  • Avoidance (people regard security as inherently dangerous, unnecessary or even harmful).

— 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 security culture, applied to the entire workforce, should be seen as a major tool to deal with the threat from insiders. [6].

— Because nuclear security at a facility has several important off-site stakeholders, understanding their perceptions, beliefs, and attitudes is central to an effective onsite security regime and to teamwork among all players. These stakeholders include law-enforcement agencies, response forces, first responders, and local communities. An assessment should gauge the extent to which a specific facility or other nuclear-related activity is culturally compatible with such offsite players.

The unique features of security culture and its assessment must not erect an impenetrable wall separating it from safety, its counterpart within the organizational culture. Safety and security should reinforce each other in pursuing the common objective of protecting people, society and the environment. Leaders must build bridges between the two fields, giving rise to a cooperative method of culture evaluation leveraging the commonalities between them.

3.3. SECURITY CULTURE INDICATORS

Ref. [1] assigns indicators to the characteristics of nuclear security culture that can be used to help assessors in measuring the culture and identifying practical ways to improve it. The main purpose of using indicators, however, is to stimulate thought and continuous learning rather than prescribe specific actions. Security indicators constitute a framework under which to facilitate change and development, promoting wanted and discouraging unwanted behaviour.

Introducing security culture indicators for self-assessment will encourage managers to reflect upon security culture and expand their awareness of the areas being measured. Appendix II lists security culture indicators to illustrate each of the 30 characteristics of nuclear security culture included in the IAEA Model. Thoroughly reviewing these indicators could be used by managers to reflect on the state of nuclear security, identify human-factor-related gaps in the security system, and take corrective measures, even without undertaking a full scope self-assessment. In other words, self-assessment is a step-by-step process from simple self-reflection to more sophisticated tools. Such a quick look, however, full self-assessment should it become necessary to check whether the original diagnosis was correct, the measures adopted by the management really worked, and the organization is on the right track toward enhancing its nuclear security culture.

Some organizations still regard 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 people's thinking about what constitutes a good foundation for security. Security culture indicators perform four main functions:

- Monitor the level of security awareness in the organization;
- Determine and improve tools and procedures for mapping security;
- Provide guidance for making a strategy to improve security;
- Motivate the management and staff to take any actions necessary.

Appendix II groups indicators around the relevant characteristics of the security culture model. Some of them are generic by nature and should be treated as samples or illustrations that help each organization tailor a self-assessment project to its needs. Additional indicators should be developed reflecting the profile of the organization and its activities. To this end, indicators in Appendix II can be modified to address, for example, a site'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. Likewise, a self-assessment project for users of radioactive sources or transport operations may need a set of specific indicators which would reflect a carefully defined risk-based and graded approach for such organizations. Such new task-specific indicators — if there is a clearly recognized need for them — should be elaborated by a team of experts and their introduction approved by the management.

A security culture improvement 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. At the same time, it should be understood that indicators cannot reveal underlying attitudes, and therefore follow-up analytical work may be necessary to provide insights into how to improve. A combined use of several assessment methods helps identify root causes while facilitating the search for solutions.

Assessors can develop additional indicators based on specific criteria such as:

- The indicator is cost-effective and reliable.
- The indicator is relevant and measures what it is intended to measure.
- The necessary data are available or can be generated.
- The indicator is not susceptible to bias or manipulation.
- The indicator is easily and accurately communicated.
- The indicator is interpreted by different groups in the same way.
- The indicator is broadly applicable across the organization's operations.
- The indicator can be validated.

Also, it is evident that history, traditions, and management practices often leave a distinct imprint on security arrangements, and particularly on security culture. Security culture indicators can be adapted to specific circumstances, helping ensure that they remain effective and consistent in diverse settings. Adjusting and modifying the indicators supplied in Appendix II will help staff perform self-assessments while encouraging national stakeholders to accept the findings.

4. SECURITY CULTURE SELF-ASSESSMENT PROCESS

As noted above, self-assessment is a step-by-step process that can be initially limited to a review of indicators by the management against available observations, document review, and other sources to provide insight into the state of security culture. If, however, the decision is made to launch a full-scope self-assessment, 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 unearthing their root causes is yet another option for selecting security culture characteristics which may be at risk. A narrowly focused self-assessment must not preclude a wider scope self-assessment campaign if deemed justified.

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, it would be useful to start the self-assessment by examining some of these qualities and their derivatives, but above all their cultural roots (see Appendix V for a possible

scenario). Cultural change takes place through a long-term process, meaning that the management and staff must keep improving culture on a continuous basis. As security culture must be periodically assessed to track progress and adjust programmes, it is beneficial to institutionalize this activity inside the organization. A standing framework can include placing a senior manager in charge, periodically disseminating information about the status of security culture, and grooming a core group of staff members to undertake subsequent assessments.

The cost of the self-assessment programme should be continuously estimated and factored into the organization's budget. The costs include computer use; the fees for outside consultants, if needed; printing of survey forms and other documents; and time spent by staff members 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. Self-assessment is an investment in better security. Still, it can be difficult to quantify the tangible benefits, at least from a short-term perspective.

A prerequisite for successful self-assessment is ensuring confidentiality for its participants and conducting self-assessment on a voluntary basis. The ways in which confidentiality might be breached should be carefully considered before data collection begins and explicit strategies be put in place for protection. The principle of voluntary participation is vital to obtain frank and sincere answers.

Upon completion of the preparatory work, the process unfolds through six stages (See Figure 3).

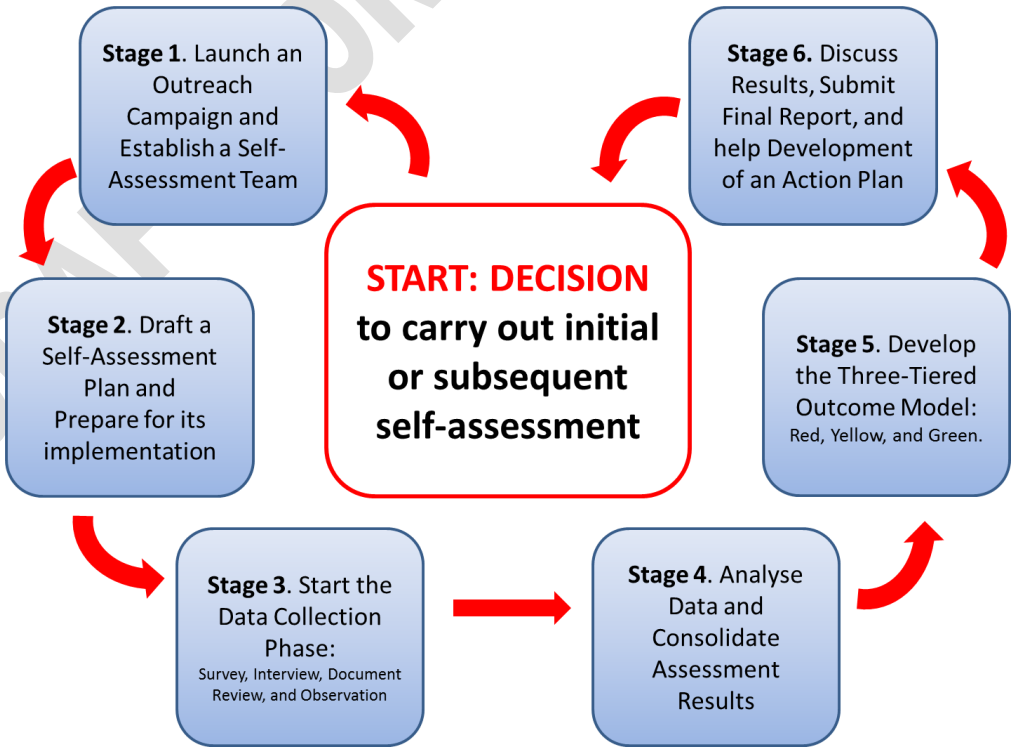

Figure 3. Six stage process of self-assessment of nuclear security culture.

Stage 1. Launch an Outreach Campaign and Establish a Self-Assessment Team. An important initial step is building commitment throughout the organization. Self-assessments commonly run into problems because of misunderstandings or apathy. To be effective, senior management must be seen as having initiated and supported the process. A directive from the head of the organization is a useful vehicle for sending this message. Such a message should state the assessment's purpose, outline the procedure for carrying it out, and explain how the results will be used. Senior management must visibly involve itself throughout the process rather than delegating responsibility. Concurrently, all senior managers must grasp 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 assessment.

A self-assessment team is established consisting of staff members who represent different departments and are familiar with the procedures for conducting such a review. A staff member with practical experience in appraising nuclear safety culture would be very helpful as a member of the team. The first several assessments will 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 diverse enough 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 to Implement It. The team and senior management work together to develop a self-assessment plan spanning the entire period of this process, paying due attention to the need to minimize the cost and avoid organizational disruptions. Methods to be included in the plan depend on several variables, such as the time allocated for its conduct, the availability of team members to perform their assessment functions, and budget considerations. These methods are broken into two categories: (1) non-interactive methods (surveys, document reviews and observations) and (2) interactive methods (individual interviews and focus-group discussions).

All of 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. Though triangulation does produce data drawn from multiple points of reference, it remains somewhat subjective. All abovementioned tools are important, but one recommended option to start with is combining non-interactive methods with interactive methods, for example by carrying out a survey followed by a set of onsite interviews to fill in possible gaps, clarify ambiguities, and generate qualitative data. Other options are possible and the choice is up to the Self-Assessment Team.

Stage 3. Data Collection After explaining to the organization's staff the objectives of the self-assessment, pointing out that it will focus on attitudes and behaviour, the team launches the evaluation. One possible scenario is to conduct surveys, then follow up with interviews, while at the same time continuing a search for relevant information from document reviews and observations. The rationale for this stage is to get insight into the state of nuclear security culture or its key aspects, helping the team determine which areas warrant further scrutiny and follow-up action.

Stage 4. Analyse Data and Consolidate Assessment Results. The team next analyses and integrates the results from the survey, 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 must be undertaken at the level of conclusions, not beforehand. Results which may contradict each other need to be double-checked and clarified through all available means.

Stage 5. Develop the Three-Tiered Outcome Model: Red, Yellow, and Green. The next step is to develop a Three-Tiered Model of Self-Assessment Outcome. It would be misleading to quantify the extent to which the results meet the indicators. Instead, a simple scale at three levels lays the groundwork for identifying weaknesses and strengths. The green level would signify good performance. It would show what needs to be reinforced to keep up the momentum. Yellow would signal that despite some positive elements, certain gaps must be dealt with. Red would indicate serious problems that must be addressed as a priority.

Stage 6. Discuss Preliminary Results Throughout the Organization and Submit Final Report for Developing a Follow-up Action Plan. The team communicates the security culture profile to the organization, requests feedback, and submits its final report. In developing a plan, it is important for the management to go beyond visible behavioural artefacts to the deeper, intangible tiers of the culture. By identifying inconsistencies and conflicts between behaviour, practices, and policies and the guiding principles, beliefs, and attitudes, the plan's drafters address the underlying causes of deficiencies and problems. This approach enables the organization to upgrade nuclear security culture after the assessment.

After the plan is finalized, senior management briefs the organization on its content. In addition to communicating general information to the entire workforce, leadership makes specific assignments designed to improve security culture. Senior management keeps lines of communication open should any parts of the action plan need to be clarified. Follow-up assessments combining old and new indicators can help identify trends while assuring that the action plan is helping enhance nuclear security culture.

While the action plan will set forth specific actions to address cultural weaknesses, achieving sustainable improvement may require, for example, other arrangements:

1. Ensuring that management systems adequately support security culture and that managers are committed to its continuous improvement.
2. Including security requirements in recruitment, evaluation, and promotion of employees.
3. Continuing to provide training sessions and briefings on security and security culture.
4. Including security culture issues in regular audits.
5. Making sure that newcomers to the organization are familiar with its traditions of and requirements for security culture.
6. Integrating security culture issues into the business planning process.
7. Keeping the organization informed of security culture developments in other organizations and sharing best practices, if appropriate.
8. Including security performance and security culture indicators in evaluations of employees and managers.

5. METHODS OF SELF-ASSESSMENT

5.1. SURVEYS

Surveys provide a convenient way to obtain input from a large number of employees. Surveys are easy and quick to complete, helping minimize work disruptions while encouraging a high response rate. This method provides clear and straightforward data because anonymous respondents can express critical views without fear of adverse consequences. See Appendix III for a step-by-step guidance of survey conduct.

Surveys are important to self-assessment because, in addition to quantifying current perceptions, they establish a baseline for tracking changes over time. Hence, some key indicators from the initial self-assessment must be reused in subsequent surveys. Also, surveys enable large-scale reflection on

selected characteristics of security culture, helping the leadership compare responses from different groups and strata of the organization to identify pockets of cultural strength and weakness.

Respondents to a survey can be asked to offer comments on the survey, particularly if they neither agree nor disagree with any statements in it or have something else to say. Their comments are a valuable tool at any stage of the self-assessment. However, a note of caution is in order: given the large number of responses demanded in the survey, writing fatigue may limit the number of comments.

The list of security culture indicators in Appendix II helps illustrate how each characteristic in the IAEA Model (See Figure 1) should ideally evolve to improve the nuclear security culture. These indicators, in addition to any new ones suggested by the self-assessment team, furnish the basis for survey statements with which respondents can express their agreement or disagreement. While some indicators can be used in the survey as they stand, others may need to be transformed according to certain criteria (See Appendix III for specific examples):

1. Statements should concentrate on a single topic because some if not most security culture indicators either focus on multiple topics or describe a multistage process to which respondents cannot give one single answer.

2. Certain indicators may need to be personalized to concentrate on strictly individual attitudes.

3. While transforming indicators into survey statements, special attention should be paid to such qualifying adjectives and adverbs as “adequately”, “well-defined”, and “reasonably” which require respondents to exercise individual judgment and thus may introduce ambiguities in the absence of clear definitions. On the positive side, they can encourage participants to offer much-needed comments. Whether to retain, modify, or delete such terms in survey statements is up to the discretion of the Self-Assessment Team drawing up the survey.

A prerequisite for regularly held self-assessments is to involve a full range of stakeholders in reasonably large numbers. The first survey supplies an overall picture and lays the groundwork for an action plan, a vehicle for improving nuclear security culture. Since indicators are highly diverse and specialized, the challenge for the first survey team is to select metrics with which most respondents are reasonably familiar. Subsequent self-assessments can be structured differently, or may include concurrent surveys that target relevant professional groups separately. For example, one survey could evaluate security personnel and the other non-security personnel. Or, one could evaluate managers and the other non-managers. Other options are possible to evaluate individual characteristics.

There are several pitfalls to be avoided when conducting surveys. They are:

— There are too many statements, fatiguing respondents.

— Instructions for completing the survey are inadequate.
— Respondents lack the knowledge and background information to respond to some statements.
— Respondents do not feel that their anonymity is protected.
— The purpose of the survey is not explained.
— Statements are open to misinterpretation.
— The survey is carried out when the staff is too busy to give it full attention.

Piloting surveys before formally administering them helps reveal unclear or confusing terminology, ambiguities in question design, or unjustified assumptions within the survey design. A pilot group should consist of 12–15 individuals representing a cross-section of the respondent pool.

See Appendix IV for histograms as a graphic representation of survey results and Appendix V for a possible scenario of survey conduct.

5.2. INTERVIEWS

Interviews play a significant role in cultural assessment because they allow for flexible questioning and follow-up questions. This eases the task of getting at the deeper tenets of an organization's culture. See Appendix VI for step-by-step guidance of interview conduct and other relevant information. Interviews also help the leadership:

— Compile a differentiated view of the performance of a facility, and of activities that bear on security;
— Determine the degree to which the staff formally and informally accepts and understands security-related policies, processes, and procedures;
— Explore security-related social norms, beliefs, attitudes, and values among the management and staff, as well as the relationships among important traits.

Interviews allow for personal contact between an interviewer and a respondent, ideally fostering an unconstrained flow of information. Interviewees, who need to be carefully selected by their experience, work positions, and skills, can give specific examples of past practices that they have seen done or heard about and even supply explanations that would provide a clue to people's insights into their beliefs and attitudes. Such discussion of past and current practices would be a good theme to keep the interview going. Face-to-face interviews can be divided into three broad types: structured, semi-structured, and unstructured. Of the three, structured interviews involve asking a series of closed questions. They are essentially quantitative surveys completed orally. They provide few benefits compared to surveys, except for compelling respondents to take part in organizations where methods like surveys are new or unpopular.

Semi-structured interviews allow evaluators to discern the context surrounding the security regime. For example, a general question to start with might be: "What is your personal role in and

contribution to maintaining or improving nuclear security in the organization?" Through positive verbal and nonverbal cues, respondents are encouraged to present their story and elaborate on their responses. Semi-structured interviews have some pre-formulated questions or themes, some of which may derive from a preliminary review of the survey results or from previous experience with security incidents. It generally benefits interviewers to prepare an informal "interview guide" listing groupings of topics and questions that can be asked in different ways for different participants. This helps the interviewer focus on the topics at hand while tailoring questions to the self-assessment goal.

Ideally, interview guides are continuously evolving tools. Questions are developed, tested, and refined based on what one learns from asking people these questions. To this end, members of the assessment team share the results of each interview with one another prior to subsequent interviews. Cross-fertilization helps them (a) forecast what kind of discussion emerges when certain questions are asked and identify questions that need to be refined; (b) share experiences from previous rounds of interviews to improve performance at subsequent sessions; (c) identify future interviewees based on recommendations from past ones; and (d) reflect on the interviewer's role, preconditions for face-to-face contact, and behaviours encountered during interviews in order to make adjustments and avoid mistakes. The breadth and depth of the assessment team's experience determines how much use it makes of semi-structured interviews. Unstructured interviews have neither the questions nor the answer categories predetermined and require much more special skills from interviewers. The focus on security is highly elusive and their output is difficult to interpret.

Focus-group sessions are more effective for exploring broader security-related issues. They also yield a large amount of information over a relatively short period. Compared to individual face-to-face interviews, group sessions have the advantage that interactions within the group often prompt and sustain discussions with minimal input from the interviewer. Group members share their experiences, views, and attitudes about 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 is to facilitate discussion while recording key points that emerge from the discussion.

Training and briefings for interviewers should ensure that they behave respectfully while showing empathy and open-mindedness. A major challenge during interviews is establishing trust and providing credible assurances of anonymity. Failing that, there is a risk that interviewees will be selective in their responses. Efficient note taking is a vital skill for each interviewer to master before launching the assessment campaign. More tips for developing interview skills can be found in Appendix VI.

5.3. DOCUMENT REVIEW

Document reviews can take place prior to self-assessment to familiarize the team with past security incidents, their root causes, and corrective measures taken, or as a tool during the process of self-assessment. The foremost purpose of document review is to determine if there is a necessary and sufficient policy and procedure basis for promoting and sustaining a strong nuclear security culture. A pattern of incidents or near misses found in documents can help narrow the focus for the self-assessment. See Appendix VII for step-by-step guidance of document review.

There are three types of document review. The self-assessment team selects the one that best fits its needs. Reviews can inquire into (a) the *literal meaning* of documents, helping the team determine how the document's framers intended for certain work to be carried out; (b) *interpretive meaning* that goes beyond the document's literal wording into the overall context within which it was formulated; and (c) *inferences* that provide wider context and an opportunity to achieve far-reaching conclusions. For instance, recurrent security breaches identified in documents and follow-up actions may point to problems with leadership performance, discipline, the compliance culture, or the learning process. Reviewing the words written on the page is necessary but insufficient to unearth such pitfalls.

Documents under review can be broken down into the following categories:

- Vision and mission statements;
- Policy statements on security;
- Arrangements for security, including assignment of responsibilities;
- Instructions for handling employee concerns, including those relating to security;
- Documents on resource allocation and qualification requirements for personnel who deal with security;
- Procedures for recruitment strategies, especially in relation to security;
- Documented training activities, with special emphasis on security, including training curricula, certification, rates of attendance, feedback, and instructors' qualifications; and
- Leadership statements, general meeting agendas, and any other information deemed appropriate in the specific assessment circumstances.

Document reviews can supply insight into how management sets its priorities and how it intends for its policies, programmes, and processes to operate in practice. Combined with surveys and interviews, a document review helps evaluators 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.

A document review is a labour-intensive process with administrative limitations. Before the assessment team decides to use this method, it must determine whether top management can make

classified documents available to the team, and whether the information gained from the review can be made available to the entire staff in interim and final reports.

5.4. OBSERVATIONS

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, time-tested, commonplace tool for managing security. The general principles of conducting observations include the following:

- The preliminary plan for observation emphasizes the most important objects and stages of surveillance.
- Observation does not disrupt the work process and schedule.
- Observation of the same phenomenon or action conducted by several persons who compare and consolidate their conclusions yields better results.
- Observation is systematic and draws on past observations.
- Previously recorded observations are often more reliable than observations conducted in the midst of a well-publicized self-assessment campaign.

There are two basic approaches to observations as a tool of security culture self-assessment: fact-based management observations and opinion-based cultural observations. Though observation is mostly about patterns of behaviour as manifestations of beliefs and attitudes, it is important to continuously monitor the completeness and functionality of the security management systems. Appendix IX provides a list of indexes to accomplish this task. These indexes can be regularly used by managers as a check list requiring from them “yes” or “no” answers. The benefit of this fact-based approach to observation is that it provides specific guidance as to what to observe in the management systems which is security relevant and have 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.

The second approach is about observing the elements of culture either directly (e.g., is the staff complying with procedures?) or inferred from observations (e.g., what values and beliefs do staff members express?). In this sense, observations can be used to vet findings that arise from surveys and interviews carried on during the triangulation process. Cultural observations are different from observations measuring the staff’s performance of assigned tasks. The latter determine how consistently written policies and procedures are executed, whereas the former probe normative standards and expectations.

Cultural observations are broken into passive and active types. The former limits the observer to just watching persons of interest and recording the results. The latter includes some kind of interaction by asking questions or requesting clarifications. Such enquiries can concentrate on specific actions or patterns of behaviour just observed. For example, why this particular security procedure or action was implemented, what implications would be of failing to implement them and many others.

The value of observations is that they do not require an underlying hypothesis that can introduce bias and distort the assessment's results. They provide valid information while revealing direct evidence of the truth of a given proposition, inference, or conclusion. As with other methods, however, the self-assessment team must remain cautious about over-generalizing from observations. Rigorous self-assessment involves the use of numerous observations of different people in different areas across the organization, helping generate valid information.

Observation can help not only to understand data collected through other methods (surveys, interviews, document review), but also to design questions for those methods that can provide valuable insights into the phenomenon being studied.

Particularly important are observations made during general meetings attended by managers, staff members, and contractors. Below is a sample list of items to be observed:

1. Do managers or meeting chairs refer to nuclear security standards and expectations?
2. Is there evidence that the staff takes ownership of security? Do attendees suggest solutions and ideas?
3. Do staff members and contractors with security expertise actively participate?
4. Do attendees from different professional groups express their views and interact with one another openly?
5. Are any assumptions about risk and other security-related matters questioned or confirmed?
6. Are people's contributions to better security publicly recognized and praised?

Observations are related to many other activities in nuclear facilities. Of particular importance are:

— Shift changeovers;
— Routine interdepartmental meetings;
— Pre-job briefings by supervisors;
— Post-job reviews; and
— Team meetings and project management conferences.

The observation process will yield results if observers: (a) take notes while observing, or reserve time to take notes immediately afterward; (b) combine formal observations of events and scenes with less formal interactions; (c) use brackets in their notes to distinguish descriptions and interpretations from reportage of simple facts; (d) regularly review their notes to synthesize insights into cultural elements. A major limit on observations is that people commonly behave differently when being watched. The observer becomes part of scene being observed. Also, it may be difficult to guarantee the anonymity of personnel under observation. The use of video cameras, for instance, for continuous observation of a particular individual or a group is subject to national laws and internal regulations. (For more on observation, see Appendix VII)

6. CONDUCTING THE ANALYSIS

The analysis stage is critical for comparing and integrating the findings of assessment tools. Without conducting an analysis, the team is at risk of merely reporting what its members have been told and presenting a factual summary. Self-assessment starts as a fact-based process but must go well beyond the facts. 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. Organizations' management expect to be able to draw upon the insight of the self-assessment team to search out and identify symptoms, uncover patterns, and identify underlying problems before they surface.

Analytical thinking can occur throughout the entire data-gathering process. However, a distinct analysis stage is highly recommended; this may be as short as half a day in a small organization and appropriately sized project, or it may require multiple days to fully explore all the issues in a multi-unit organization. An analysis session with the participation of the entire self-assessment team ensures that all members have a chance to share their views and add what value they can. It is also important to have preliminary analysis sessions before the team has finished gathering all the facts, especially after the survey. That way, there is still time for modifying an interview guide, re-interviewing or adjusting interview requests to pursue the questions that emerge during preliminary analysis. The analysis process is undertaken in several consecutive steps:

Step 1. Organize a brainstorming session for all team members (for a preliminary or final analysis session) to identify issues which have emerged from the use of self-assessment tools. Brainstorming is effective in deciding what the issues are – a moderator simply writes all ideas for issues on a whiteboard. The original list is likely to shrink to a more manageable length as debates continue.

Step 2. Discuss the revised list and revamp it. Once a list has been established, team members discuss each issue and offer their perspectives. It is quite possible that conclusions reached

about one issue may merge it with others, create new issues, or cause others to disappear. The list of issues is a moving target until the end of the process.

Step 3. Develop hypotheses to explain identified problems. Team members must look for the root cause or causes and find out why these issues exist, whether they can be validated through other means, and how widespread they are in the organization.

Step 4. Review the hypotheses, test them against known information, and seek new evidence by re-interviewing relevant individuals among other methods. As a result, team members will have one or more related hypotheses that they believe to be correct, inasmuch as they match the available evidence and have withstood any tests of reasonableness and attempts to verify them.

Step 5. Formulate conclusions and explain why the issue was selected, its cultural roots, its relevance for nuclear security and what needs to be done to address it. This outline is designed for inclusion in the final self-assessment report which the team will develop and submit upon completion of the analysis stage.

Step 6. Develop a visually distinct three colour model (red, yellow, green) of conclusions at which the self-assessment team can arrive. Red includes identified weaknesses requiring action; yellow reflects concerns regarding issues which can potentially become problems; green contains strengths of the organization which must be maintained and used to achieve the objective of a more effective nuclear security. Cultural change is slow-progressing, so it would be prudent to focus – particularly if this is the first self-assessment effort – on just a few key items in such a chart.

Below are two case studies to illustrate the suggested analysis methodology:

Case Study 1: Assume that in a survey a sizeable number of respondents 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. It sends the message that this group doubts the existence of a threat or the importance of nuclear security, the underlying beliefs and attitudes of nuclear security culture. In their efforts to understand the cultural root causes of this reaction, the assessment team reviewed responses to similar statements and comments that may provide clues. The initial list of hypotheses included: (a) inefficient lines of communication have kept management from delivering a clear message; (b) the training programme places too little emphasis on security; (c) security arrangements are a low priority in the organization's budget, downgrading its importance in the eyes of the staff; (d) policies pertaining to career advancement ignore security performance; and several others. To narrow 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: (a) inefficient lines of communication; and (b) career advancement ignores security performance. Upon further elaboration, team members agreed that because of poor coordination, management's messages about the importance of nuclear security fail to reach all workforce groups. In the absence of consistent policies and efficient use of communication channels, there is a growing trend among the workforce to relegate nuclear security to a secondary role and treat it accordingly.

Case Study 2: Conflicting responses to the same survey statement present a slightly different challenge. The self-assessment team started by determining whether perceptual fault line runs between security and non-security personnel (surveys remain anonymous, but in order to facilitate post-survey analysis, respondents are requested to check a box indicating to which general category they belong). If so, this variance between the two subcultures risks becoming a serious obstacle to effective cooperation between these two groups. It could hamper teamwork while impairing the security regime. Conflicting responses may result from a variety of other factors and phenomena, including differences of perception between non-security-related departments, between long-time employees and fresh recruits who have yet to become acculturated, and the like. Yet another root cause may be a tradition of exempting senior personnel and high-ranking visitors from burdensome and time-consuming security measures for access to sensitive areas. Such exemptions send the message to those who witness these events that senior leaders are a privileged category and care little about such security arrangements. The implication for the workforce is that security is not important. The initial list included the following hypotheses: (a) two conflicting subcultures: security and non-security; (b) new employees are slow to internalize organization's culture; (c) failure of senior management to act as role models; and (d) inefficient lines of communication. Further deliberations among team members and interviews enabled the team to delete (a) and (b). The self-assessment team agreed that the remaining hypotheses: failure of senior management to act as role models and insufficient lines of communication are interconnected and explain the split in the workforce in its treatment of nuclear security as a clearly recognized value in the organization. Appropriate conclusions were made and reflected in the final report.

Effective analysis requires an analytical framework based on interpretation. In cultural analysis, this framework must be made explicit and include knowledge of how culture operates. It means that information obtained from surveys, interviews, and other methods is to be interpreted and analysed, not treated as self-evident conclusions.

The resultant Three-Tiered Model of Self-Assessment Outcome (See Figure 4) differs from the three-color breakdown of the 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). It is possible that after comparison and consolidation, some themes originally in one colour zone of the survey be moved to another and will require different corrective actions. One important benefit of transitioning from a three-color survey scheme to the final three-color scheme is to demonstrate how the input from other self-assessment methods can modify initial conclusions by revealing deeper cultural layers of security-related successes and problems.

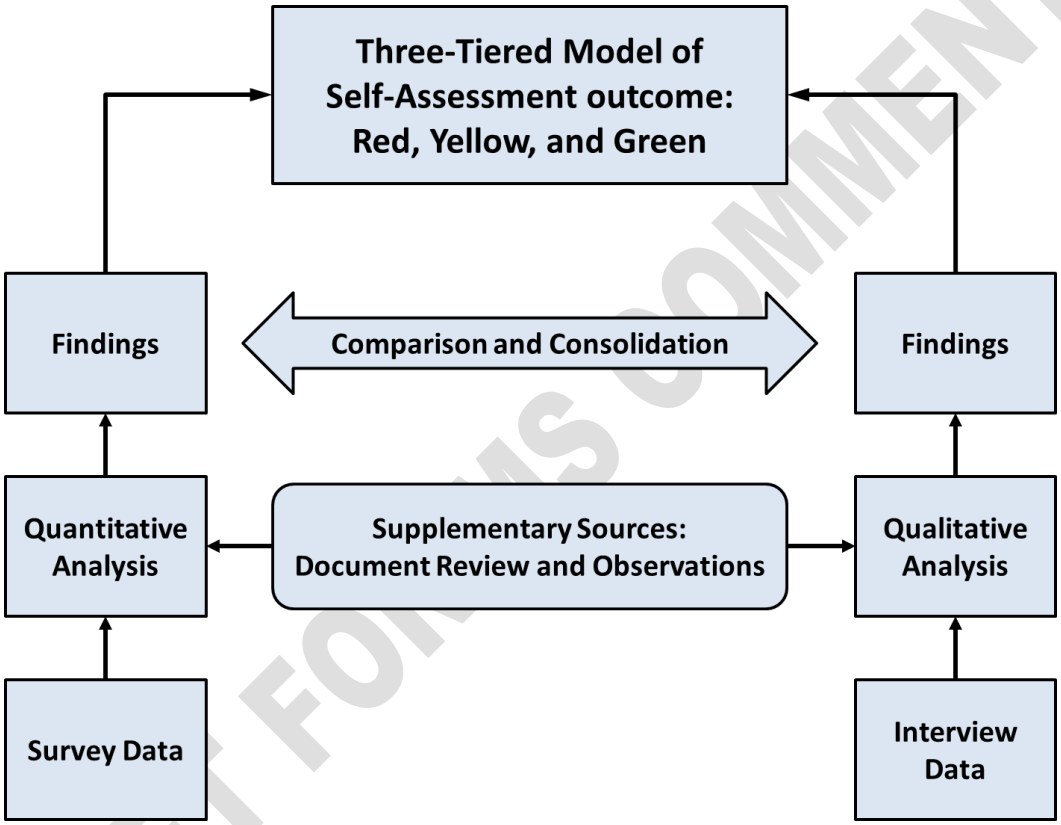

Figure 4. Use of quantitative and qualitative data for findings analysis.

Self-assessment conclusions may identify numerous problems in the organization such as overconfidence and complacency; lack of a systemic approach toward security risks; leadership and management that depend more on security technology and underestimate the role of the human factor; apathy or ignorance toward security culture; or indifference to the experience of others. Consistent use of indicators as references will help the management draw up an action plan for cultural transformation.

7. COMMUNICATION OF FINDINGS AND TRANSITION INTO ACTION

The self-assessment process culminates in a final document summarizing the results, setting the foundation for communicating key messages, providing a baseline for subsequent self-assessments, and laying the groundwork for the action plan. Given its wide scope and multiple purposes, the report should cover the following:

- Rationale for focusing on culture as a contributor to nuclear security;
- Reasons the self-assessment was undertaken, what methods were used, and who was involved;
- Basic information about the way the analysis was conducted;
- Patterns and themes that illustrate strengths and weaknesses in the culture;
- Measures for addressing issues to be explored further in the action plan; and
- An invitation to provide feedback on these or any other items.

A major purpose of the report and the communication phase is to foster a sense of ownership among the staff. This makes each person a joint custodian of the security culture. To this end, the report must emphasize the benefits of this long-term endeavour to individuals and groups, helping them transcend the customary understanding of security. Spillover benefits can include an efficient security regime, better IT security, protection of trade secrets, improved safety, reduced theft and diversion of materials across the board, reduced risk of vandalism and sabotage, improved mechanisms for control during emergencies, and less cumbersome auditing procedures.

Communication meant to elicit feedback and advance organizational learning typically occurs in several formats:

- The self-assessment team conducts an exit meeting to pass on the review's highlights to management.
- Management and the assessment team jointly disseminate the review's findings to the staff, holding face-to-face meetings, workshops, and seminars supplemented by bulletins, Intranet postings, and other social media, paying due heed to the confidential nature of some of the information, (if necessary, the final self-assessment report may have two versions: one for internal use and the other for the public domain).

The communication phase attunes senior management and the entire organization to the role of the human factor in security, helping them learn lessons and take corrective action. Interaction is a healthy part of the process. Findings should be discussed and debated rather than simply published in a report. Robust debate helps management and staff expose gaps and problems in the culture that might open the way for security breaches.

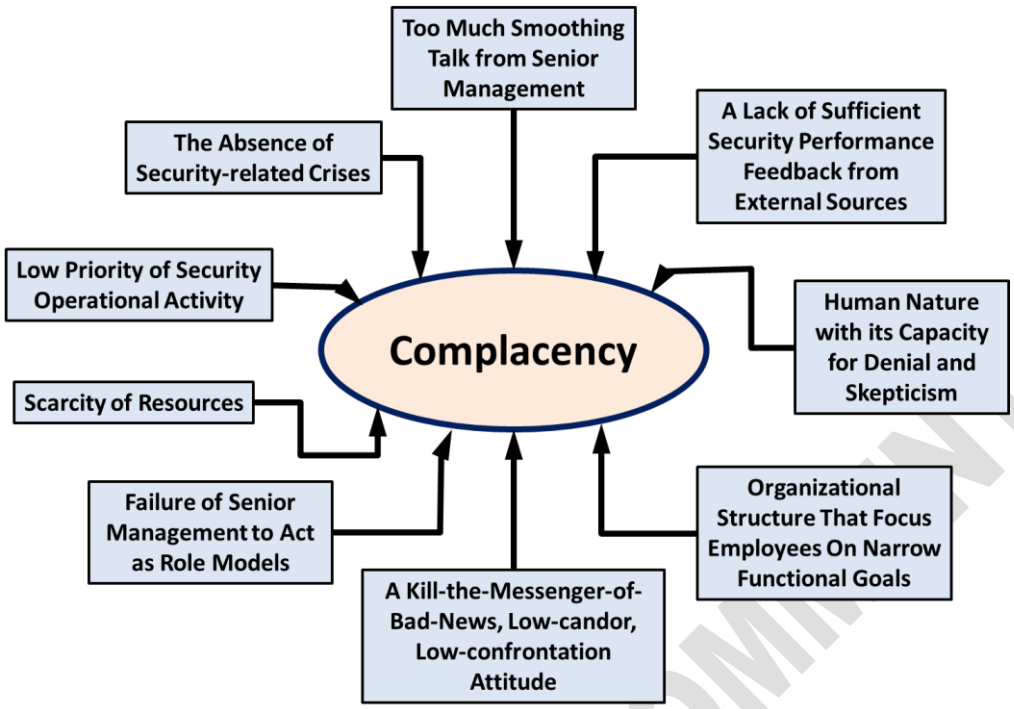

Figure 5. Root causes of complacency.

The final stage in the process is for senior management to use the assessment results to determine how to reshape knowledge and traits that are incompatible with an effective security culture. Of special importance is banishing complacency, the rationale behind cultural reform and maintenance. See Figure 5 on prospective sources of complacency.

As is the case with safety culture, over-confidence is a precursor of complacency in security culture. In both cultures, complacency is brought about as a result of good past performance, praise from evaluators and unjustified self-confidence [7]. If unchecked, overconfidence turns into complacency when oversight activities begin to be weakened and self-satisfaction leads to delay or cancellation of some important programmes.

Self-assessment is designed to diagnose signs of complacency and address its root causes. It would be imperative at this stage to focus on what may look like minor or near miss security events and tendencies to ignore them, analyse negative or borderline findings from different perspectives, and vigorously evaluate real – and not just expected – effects of ongoing improvement programmes. In this sense, periodically held self-assessment can be a powerful tool to prevent the slide toward complacency and further weakening of nuclear security regimes. This mission, however, can be accomplished only if members of self-assessment teams are carefully selected for their commitment, dedication and specific skills.

If self-assessment provides diagnosis, it is the task of the management to draw timely lessons and squarely address all identified strengths and weaknesses of culture as a vital element of its long-term strategy. Four principles should guide their action:

- *Never start with the idea of changing culture.* Always start with the specific issues besetting the organization. Only when the problems are clear should one ask whether the culture aids or hinders efforts to solve them.
- *Remember that culture is not an undifferentiated mass.* Culture varies from endeavour to endeavour. An organization can have a culture, which helps achieve one type of result but provides little help with another. This is the reason why a nuclear security culture must be investigated specifically: it cannot be assumed to exist just because the facility is performing well in other domains.
- *Think of culture as a source of strength until proved wrong.* Even if some elements of the culture look dysfunctional, remember that these may be a few weaknesses among numerous strengths. If change must be made, build on existing cultural strengths rather than concentrating on weaknesses.
- *Facilitate cultural change rather than creating a new culture.* Managers can demand or stimulate new ways of thinking or working. They can monitor compliance. But members of the organization will not internalize the new culture unless it works better and delivers benefits over time.

Drawing on the self-assessment's results, the action plan charts a roadmap for senior management to manage the human factor and instil an effective nuclear security culture. Subsequent assessments are a must to check progress and make any additional adjustments. However, the approach delineated here is that the self-assessment and its report should remain separate from the follow-up action plan for culture enhancement, which is subject to other IAEA guidance.

8. CONCLUSION

As nuclear security culture becomes a widely recognized tool in efforts to bolster nuclear security, it is imperative to introduce user-friendly, universal methods for assessing it. This can be a daunting challenge because intangible human characteristics like beliefs, attitudes, and values comprise a culture. Measuring cultural traits requires a multidisciplinary and interpretive approach. Nevertheless, assessment of security culture can draw on rich experience with evaluating organizational culture and, in particular, nuclear safety culture.

Self-assessment is not an end by itself but rather an important learning implement that helps an organization understand the reliability of the human factor and how culture influences security performance. The methodology proposed here involves large numbers of staff members at all levels.

Broad organizational participation lends itself to the validity of self-assessment findings. In addition, it widens ownership of the self-assessment outcome, facilitating implementation of subsequent improvement decisions and actions.

There is often a lag between the time weaknesses develop and an event with significant security consequences. Weaknesses tend to interact synergistically, creating an unstable security environment that exposes the organization to security incidents. By identifying early-warning signs through regular self-assessments, corrective actions can be taken in time to prevent or mitigate security breaches.

Self-assessment of nuclear security culture must be seen in its broadest context. All elements of the nuclear infrastructure—fuel-cycle facilities, research reactors, manufacturers and users of radioactive sources, transport companies—must be both safe and secure. Accordingly, evaluation of safety culture and security culture should proceed in tandem, helping safeguard human life, society, and the environment. Once instituted, this methodology will facilitate evaluations of vulnerabilities while identifying realistic requirements for physical protection. Assessment of nuclear security culture will enrich facilities—helping them transform the human factor from a problem to be overcome into an asset to strengthen security.

APPENDIX I: NUCLEAR SECURITY CULTURE AND THE IAEA MODEL

Scholars use the word *culture* 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 distinctive approach.

Organizational culture, of which security culture (like its counterpart, nuclear safety culture) is one of several subsets, comprises broad guidelines rooted in organizational practices learned on the job. The reason organizational culture was largely ignored until the 1970s as an element of an organization's performance is that it encompasses values that are taken for granted, along with underlying assumptions, expectations, collective memories, and definitions present in any organization. The business and academic communities now unambiguously acknowledge that is represents a significant factor in performance, productivity, safety, security, compliance and personnel discipline. Accordingly, several methodologies have been developed to evaluate organizational culture and track its evolution over time.

Security culture is a vehicle to improve human performance at nuclear facilities and organizations exposed to outside and insider threats. Most security lapses result from human failings such as low motivation, miscalculation, ignorance or malice. However, breaches of security among personnel—both unintentional and intentional—do not take place in a vacuum. In most cases they result from a broken organizational culture. The reverse effect is possible as well. Developing a more effective security culture can spill over into the overall organizational culture, improving performance across the board. When we set out to improve the human component by promoting a security culture, we set out to cultivate habits, attitudes, and traditions that favour security over lesser concerns and priorities.

This multidisciplinary approach encompasses a variety of managerial, organizational, behavioural, and other tools. The leadership need not choose between a technology-centred and a human-centred security design. Rather, security arises from the interplay among technology, culture, and people. These elements cannot be divorced from one another. In other words, a major objective of security culture is to facilitate human interaction with technology—both hard and soft, covering procedures and regulations—in security-critical systems with a view toward helping staff members recognize problems, identify emergent events, and anticipate patterns that might lead to a security breach. The more sophisticated security technologies and arrangements are, the more important the people are who design, operate, maintain, and improve the hardware.

The IAEA security culture design is based on Edgar Schein's model of organizational culture 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 repercussions of slipshod human performance. There are many synergies between safety and security, two domains that overlap within

the overall organizational culture. Accordingly, the safety model provides a ready-made analytical framework for exploring and promoting nuclear security culture.

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." [8] Applied to security, a subset of organizational culture, its essence is jointly learned, relevant values, beliefs, and assumptions that become shared and taken for granted as a nuclear facility operates at an acceptable risk and compliance level. To paraphrase Edgar 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."[9] Schein proposes that culture exists in layers comprising underlying assumptions, espoused values, and artefacts. Some layers are directly observable. Others are invisible and must be deduced from what can be observed in the organization. It is critically important to probe the latter, as they constitute the driving force for human behaviour.

Cultures, then, stem from 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 observable forms such as documents and behaviours. 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 the ultimate goal of security culture assessment is to fathom underlying assumptions looking at observable artefacts.

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 compose the third and observable layer. Physical protection equipment, people's behaviours, written documents, and work processes are all visible artefacts of security culture.

Using Edgar Schein's three layers of culture, the model for nuclear security culture reproduced in the IAEA Implementing Guide [1] breaks the artefacts of culture into three parts, for a total of five elements (see Figure 1). They are: (1) beliefs and attitudes (corresponding to what Schein calls "underlying assumptions"; (2) principles for guiding decisions and behaviour (corresponding to what Schein calls "espoused values"); (3) leadership behaviour (specific patterns of behaviour and actions designed to foster more effective nuclear security); (4) management systems (processes, procedures, and programmes in the organization which make security a top priority and have an important impact on the security functions); and (5) personnel behaviour (the product of the leadership's efforts and of properly working management systems).

(1) Beliefs and Attitudes

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. There is nothing on which to build an effective nuclear security culture without a strong substructure of convictions about threats. Efforts to instil such beliefs and attitudes must 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 a must. Two major sources of such beliefs and attitudes are the site's leadership and individuals' work experience. Leaders must lead by example to etch security-related ideals within the culture, shaping the staff's habits of mind and deed.

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. In other words, the whole workforce, not security specialists alone, must assume the site is vulnerable. According to Schein, "the essence of a culture lies in the pattern of basic underlying assumptions ["beliefs and attitudes" in the IAEA model], and you understands those, you can easily understand the other more surface levels and deal appropriately with them." [8]

(2) Principles

An effective nuclear security culture requires 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 be immersed in these principles, and there must 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. They are all essential, but learning and improvement stands above because it is key to implementing the other principles. Depending on the institution's profile and specific needs, these principles may include a wide variety of training modules, including initial training, periodic training, ongoing programmes, ongoing assessments, and quality assurance vis-à-vis training and trainers.

(3) Leadership Behaviour

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 language, and the guiding principles. The culture therefore tends to mirror the intentions, specific actions, and priorities of the upper levels of leadership—provided leaders understand and execute this function.

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 see to it 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.

(4) Management Systems

There is little unique about the seventeen management systems listed in Figure 1 of the main text, except for two: (a) visible security policy and (g) information security. Most others overlap with the more generic systems that constitute the overall organizational culture. 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 must clearly understand "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 executed.

(c) Quantifiable measures of performance, with associated goals, are an essential tool for communicating management's expectations and assuring the staff reaches 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 must be 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 must implement classification and control measures to protect sensitive information.

(h) The equipment comprising a nuclear security system requires periodic maintenance, as well as occasional modification and replacement. The intended function of the system must never be compromised. If part of the system must be temporarily removed from service, measures must be put in place to compensate.

(i) Any security barrier or procedure can be defeated by insiders. Processes for determining staff members' trustworthiness and mitigating insider threats must be in place.

(j) The security function demands the same degree of rigor, control, and assessment as any other major programme area. Performance in this domain should be documented to earn trust and support for the organization and the people in it.

(k) Inadequate management of change to equipment, procedures, structures, and roles or personnel poses problems. The organization must institute procedures to understand, plan, implement, and reinforce change as it applies to security.

(l) Processes must exist for reviewing experience and applying the lessons learned to improve future performance.

(m) Contingency plans must be drawn up to guide the response to malicious acts or to equipment or human failures within the site.

(n) There must be 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) Nuclear security typically involves regulatory and law-enforcement bodies. A constructive working relationship with watchdog institutions is therefore important to ensure that information is exchanged regarding nuclear security.

(p) Nuclear security requires frequent staff- and management-level communication with off-site organizations that provide medical assistance, emergency maintenance, and other services.

(5) Personnel Behaviour

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

An effective security culture will yield numerous benefits, encouraging the workforce to remain watchful, question irregularities, execute its work diligently, and exhibit high standards of personal and collective accountability. It is no panacea, but it can effectively contribute to a vibrant and robust security regime spanning the entire workforce. It helps the institution keep pace with a threat milieu in which risks are too numerous to predict—even for the most farsighted leader.

APPENDIX II: SECURITY CULTURE INDICATORS FOR SELF-ASSESSMENT

The objective of this list is to evaluate the characteristics of nuclear security culture at the facility level by using these indicators as references for the actual characteristic's performance. 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 into 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. Printed in bold are indicators listed in the Implementing Guide [1], followed by suggested additional indicators. 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.

I. Management System

a) Visible Security Policy

A policy document is needed in an operator's organization which 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:

1. **A nuclear security policy is established for the organization, is posted in facilities and offices, and is familiar to staff.**
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.
11. Regularly held management meetings at the organization adequately 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 policy to encourage implementation of the nuclear-security policy, with some 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. 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

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:

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 and/or training sessions.**
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 (design basis threat, or DBT) against which nuclear and radioactive material should be protected is determined and well understood by all parties involved in designing, applying, and evaluating the security measures.

12. Systems are in place to examine and make use of the synergies between safety and security.

c) Performance Measurements

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:

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 the 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, management walkthroughs, reporting of issues, indicators, trend analysis, benchmarking, industry experience reviews, self-assessments, and performance assessments.

d) Work Environment

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:

1. **The work environment is conducive to high standards of performance (e.g. standards of housekeeping, timely provision of equipment and tools)**
2. **Staff is 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 manned security posts. Special attention is paid to periods of reduced activity such as back shift 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.
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.

e) Training and Qualifications

An effective nuclear security culture depends upon staff having the necessary knowledge and skills to perform their functions to the desired standards. Consequently, a systematic approach to training and qualification is required for an effective nuclear security culture.

Security Culture Indicators:

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 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 requirements for reporting security violations.**
9. Systems are in place to ensure procedures and practices learned in training are applied in practice.
10. Leadership skills and best practice in security are included in training programmes for managers and supervisors.
11. Management is 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. Management is committed to participating in nuclear-security courses.
16. Training materials include best practices and lessons learned from security breaches.
17. Staff members can provide feedback to 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 best practices with other organizations.
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.

f) Work Management

All work must be suitably planned in order to ensure that nuclear security is not compromised.

Security Culture Indicators:

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 unforeseeable 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. Cyber 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. Management takes action on feedback to counter negative trends in security.
9. Minor security issues are addressed promptly.
10. Consideration is given to synergies and contradictions among 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.

g) Information Security

Controlling access to sensitive information is a vital part of the security function. Accordingly, the organization must implement classification and control measures for protecting sensitive information.

Security Culture Indicators:

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 assets 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 to the sensitivity of the asset.
7. An information and computer security function is established, funded, staffed, and visible.
8. Management is fully committed to and supportive of computer-security initiatives.
9. Documented IT-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.

h) Operations and Maintenance

Nuclear security system equipment will require on-going 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 must be removed from service, compensatory measures are in place.

Security Culture Indicators:

1. **Operation and maintenance are performed according to approved procedures and vendor schedules to ensure that design requirements are not compromised.**
2. **Checklists/detailed procedures are used.**
3. **Measures are taken as compensation when security equipment is taken out of service for maintenance or when breakdowns occur.**
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 defined by the DBT.
7. Work orders for repair and maintenance of security equipment and hardware are performed expeditiously.
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 is used in 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 are provided to hold workplace forums for discussing issues of mutual interest to operations and maintenance staff.

i) Determination of Staff Trustworthiness

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 must be in place.

Security Culture Indicators:

1. **Documented staff and contractor screening processes are matched to the risks and threats associated with the specific employment roles and responsibilities. Screening must be 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/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 or criminal and aberrant behaviour.**
8. **An effective insider threat mitigation programme, coordinated among all aspects of the security and operations, is in place.**
9. The process of background checks is periodically reviewed.

j) Quality Assurance

The security function of an organization is important and requires the same degree of rigor, 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:

1. **Assessment processes are in place for the security function.**

2. **Staff throughout the organization understands that 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 (recording of formal approval, periodic and planned review, testing, lessons learned, etc.)
4. Quality-assurance measures are enforced.
5. Quality-assurance procedures are periodically evaluated against best practices for the industry.

k) Change Management

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:

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 are made of changes to confirm that the desired outcomes have been obtained.**
4. **Evaluations are conducted during planning of the change process to determine if the change affected established 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 which 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 structure that are likely to affect security, a communication process is established to inform and encourage adherence.

l) Feedback Process

An organization that can learn from its own experience as well as that of others will be able to continuously improve its nuclear security performance. In order to do this effectively, processes must exist for obtaining, reviewing, and applying experience from internal and

external sources.

Security Culture Indicators:

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.**
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.

m) Contingency Plans and Drills

The nuclear security system must 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 must be conducted periodically.

Security Culture Indicators:

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, 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 do not get 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 back shift and weekends.**
5. Contingency plans are coordinated with and linked to a relevant national strategy.
6. Contingency plans are tested not just with onsite forces but also in coordination with offsite backup forces.
7. Managers are trained to effectively deal with exceptional situations for which no procedures have been devised and when no management supervision is available.

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.

n) Self-Assessment

There must 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:

1. **A self-assessment programme is documented with a plan that defines self-assessment processes.**
2. **Identified deficiencies are analysed to identify and correct emerging patterns and trends.**
3. **Human factors methodologies are incorporated into problem analysis techniques.**
4. **Performance is benchmarked to compare operations against national and international best 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 instituted as a result of security assessments.
9. Senior management plays a visible role in the promotion, preparation, and conduct of self-assessment.
10. Organization looks upon assessments, reviews, and audits as an opportunity rather than a burden.
11. There is an established procedure to continuously monitor security culture through use of indicators to implement improvements and prevent the degradation of security culture.
12. Management measures the extent to which training programmes contribute to improvements in attitudes toward security culture.
13. Staff members and contractors can give examples when senior management initiated actions 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.

o) Interface with the regulator (and law enforcement bodies)

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:

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. Organization fully understands the regulatory body's responsibility.
6. Organization shows respect for competent authority, and its mission enjoys visible support and cooperation from management.
7. Staff members and contractors view the regulatory presence on the site positively.

p) Coordination with off-site organizations

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:

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. Offsite and onsite 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 the native language.

q) Record Keeping

Efficient record keeping is vital to the safe and secure operation of nuclear facilities as well as accurate audits and assessment.

Security Culture Indicators:

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

II. Leadership Behaviour

a) Expectations

Leaders must establish performance expectations for nuclear security to guide staff in carrying out their responsibilities.

Security Culture Indicators:

1. **Leaders have and communicate to staff members and contractors specific expectations for performance in areas that affect the nuclear security system.**
2. **Leaders ensure that resources are available to provide effective nuclear security.**
3. **Leaders lead by 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 walk-throughs, 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 seeing to it that this commitment translates into daily routine.
9. Leaders provide on-going 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 management regarding security.
13. Senior managers encourage workforce to look at other organizations or other parts of their own organization to see what they can learn from them.

b) Use of Authority

Management establishes the responsibility and authority of each position within the nuclear security organization. Authority should be clear and documented.

Security Culture Indicators:

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. Management holds people accountable for their behaviour.
6. Vigorous corrective and improvement action programmes are in place, supervised by leaders, effective management and regulatory authority.
7. Managers launch, if necessary, procedures for investigating security problems, seeking advice on the causes thereof, and improvements to be implemented.
8. Leaders must define a strategy to bring information on the current security policy to the attention of staff members and contractors.
9. If possible, senior management prevents staff downsizing 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.

c) Decision-Making

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:

1. **Leaders make decisions when the situation warrants.**

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.

d) Management Oversight

An effective nuclear security culture depends upon the behaviour of individuals, and such behaviour in turn is very strongly influenced by good supervisory skills.

Security Culture Indicators:

1. **Managers spend time regularly observing, correcting and reinforcing 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. Management appreciates the importance of security culture in the accomplishment of security tasks.
7. Management ensures that a security-conscious environment permeates throughout the organization.
8. Management monitors the personnel's coping skills, stress, and fatigue levels.
9. Management helps build trust and promote teamwork within the organization.
10. Management ensures periodic audits and updates of computer security policy and procedures.

e) Involvement of Staff

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:

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 is actively involved in 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 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 to practical problems, and mechanisms are in place to support their contributions.
7. Plans are in place to handle labour strikes without unacceptable impact on nuclear security.

f) Effective Communication

An important part of an effective nuclear security culture is to encourage and maintain the flow of information throughout the organization.

Security Culture Indicators:

1. **Leaders ensure that communication is valued and that potential blockages in communication are addressed.**
2. **Leaders explain the context for issues and 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 reinforces 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 various rules and procedures is clearly communicated and adequately explained to the personnel.
11. All are aware of a policy of clear and unhindered communications, both upward and downward, within in the organization.
12. The system of communication is regularly tested to check that managers are being both received and understood by the workforce 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.

g) Improving Performance

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:

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 just 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 management shows 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" 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-through on actions involving security related human performance.
11. Senior management ensures the analysis of events derives relevant information that can be used for improving security performance.
12. Managers and relevant staff members are aware of best practices pertaining to national and international security.
13. If deviations to a procedure are needed, there is an efficient and effective means to manage it correctly.
14. Human-factor specialists and psychologists are engaged with the organization.

h) Motivation

The satisfactory behaviour of individuals depends upon motivation and attitudes. Both personal and group motivational systems are important in improving the effectiveness of

nuclear security.

Security Culture Indicators:

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 mirror those used to reward good performance in safety and operations.
10. The leadership has taken action to make career paths in nuclear-security management career-enhancing.
11. Staff members and contractors can give examples 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.

III. Personnel Behaviour

a) Professional Conduct

All organizations involved with nuclear security need their personnel to adhere to high standards of professionalism.

Security Culture Indicators:

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 each other and interact with professional courtesy and respect.**
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 an opportunity to improve them.
7. Staff members and contractors are prepared to face the unknown and improvise, if necessary.
8. Security 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 downgrade security, even if it 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.

b) Personal Accountability

Accountable behaviour means that all workers know their specific assigned tasks related to nuclear security (i.e. what they have to accomplish by when and what results should be achieved) and that they either execute these tasks as expected or report their inability to do so to their supervisor.

Security Culture Indicators:

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.

c) Adherence to Procedures

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 resort to departing from the approved methods.

Security Culture Indicators:

1. **Staff members adhere to procedures and other protocols, such as information 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 noncompliance with the established rules for organization's 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 management.
8. Staff members and contractors show reasonable trust in and acceptance of security procedures.
9. Procedures are immediately available at all work stations.
10. Staff members and contractors avoid shortcuts in implementing security procedures.

d) Teamwork and Cooperation

Teamwork is essential. An effective nuclear security culture can best be formed in an organization where there is extensive interpersonal interaction and where relationships are generally positive and professional.

Security Culture Indicators:

1. **Teams are recognized for their contribution to nuclear security.**
2. **Staff members interact with openness and trust and routinely support each other.**
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 each other's actions and by supplying constructive feedback when necessary.
6. Professional groups appreciate each other'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 improve communications between teams.
9. Cross-training among 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 which 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 measures to maintain security cooperation between organizational units.
12. The staff members and contractors use a single technical vocabulary to achieve easy interactions.

e) Vigilance

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:

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 requirement 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 must 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 breach.

APPENDIX III: PREPARATION AND CONDUCT OF SURVEYS

TABLE III–1: ADVANTAGES AND LIMITATIONS OF SURVEY AS A SELF-ASSESSMENT METHOD

Surveys	
Advantages	**Limitations**
• Easy administration and low cost for data collection from a large number of people	• Survey respondents may not complete the survey resulting in low response rates
• Reduced likelihood of evaluator bias because the same questions are asked of all respondents	• Items may be understood differently by individual respondents
• Surveys are commonly used methods and many people are familiar with them	• Some participants may have insufficient information to respond
• Some people feel more comfortable responding to a survey than participating in an interview	• Inability to identify respondents personally and probe for additional information
• Processing of responses is a straight forward process	

Before launching a survey, the Self-Assessment Team must gauge the benefits that this evaluation tool can bring. Below is a step-by-step description of survey conduct.

Step 1: Topic Selection

Survey is usually the first major step in the self-assessment process, and is concentrated on the characteristics that are believed to be weak and vulnerable. 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 prerogative of selecting topics belongs to top 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.

Culture self-assessment is basically 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 this Appendix "adherence to procedures" is selected as the topic.

Step 2: Selection of Security Culture Indicators

If the "adherence to procedure" characteristic is chosen, Appendix II lists eight indicators for this characteristic which must be carefully considered for possible inclusion in the survey. Which of them are consistent with the nature of organization operations, will they be understood by potential respondents, and should new indicators be developed for addition? 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. The search for more indicators then moves to 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 qualification," "information security," "use of authority," "management oversight," "motivation," to name just a few. As a result, the total numbers of selected security culture indicators for the survey can optimally range between 25 and 35.

Step 3: Transformation of Indicators into Survey Statements

Some indicators are included in the survey as they stand, but others may require certain modifications for clarity and to conform to the specific nature of the organization. In transforming certain indicators the following criteria are to be observed.

(a) Statements should have a single focus because some, if not most, indicators either have multiple focuses or describe a multi-stage process to which respondents cannot give one single answer. Hence, it is helpful to select one element of the indicator most relevant to "adherence to procedure" as the centrepiece 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." From a double-focused statement to a single-focused statement.

(b) Since indicators apply to the entire organization and thus require in-depth background information which most respondents may lack, certain indicators had to be personalized to focus on strictly individual attitudes. Accordingly, indicator III (c) 5—"Organization's instructions on security are easy to follow because they are clear, up-to-date, readily 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 (organization-wide) and personalized statements. Inclusion of select generic statements makes it possible to understand how an individual respondent evaluates other people's behaviour and organization-wide management practice.

(c) While transforming indicators into survey statements, special attention must be paid to the use of such qualifying adjectives as "adequately," "well-defined," "reasonably," and others that compel respondents to exercise judgment, with unexpected consequences. On one hand these qualifying adjectives are likely to confuse respondents, while on the other may incentivize them to provide much-needed comments leading to valuable insights that clarify the cultural dimension of nuclear security.

More examples of such transformation are in TABLE III–2 below.

TABLE III–2. TRANSFORMATION OF SECURITY CULTURE INDICATORS INTO SURVEY STATEMENTS

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 management (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 unnecessary (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 witnessed how our leaders personally inspect performance in the field by conducting walk-throughs, listening to staff, and observing work being done.

Step 4: Scoring Scheme Development

It is up to the self-assessment team to determine the scoring scheme for the survey. There are numerous options, and choosing among them must take into account past surveys and methods used,

compatibility with surveys in other organizations, the management's preferences for complexity versus simplicity—especially if this is a pilot project—and other factors. The present guidance suggests a scoring system employing a 7-point scale from 1 ("Strongly Disagree") to 7 ("Strongly Agree"). This scheme (See Figure III–1) 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 judgment on a particular point and is requested to provide a reason in the comment space. This box is particularly important because it provides data subject to a wide range of interpretations. If respondents know nothing about the subject of a statement, they can tick the "Not Applicable" (N/A) box.

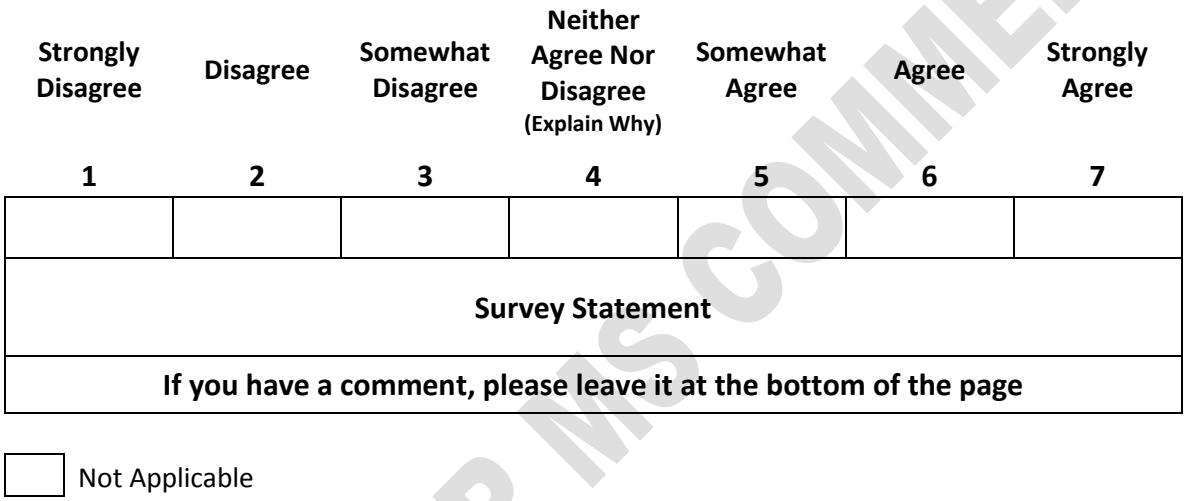

Figure III–1. Seven-point scoring scheme for self-assessment.

Other scoring options are possible. One is a 11-point scale from "Fully Disagree" (0) to "Fully Agree" (10). Its application will produce more nuanced responses from the target group. As with the 7-point scale, respondents with no knowledge of the subject matter are asked to check the N/A box. The descriptions are shown both ends only. The words in the other boxes are not added particularly. The score should be used as a weight scale.

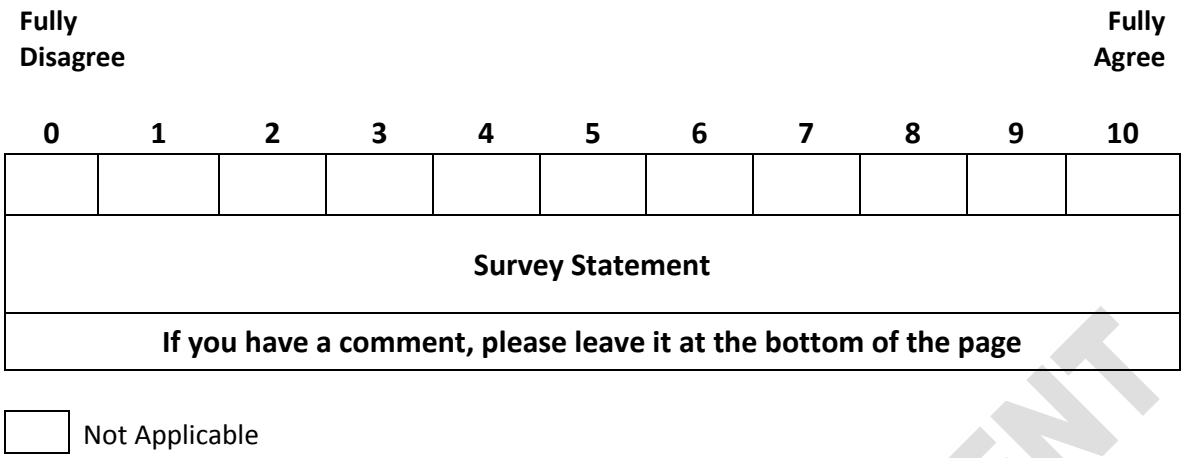

Figure III–2. Eleven-point scoring scheme for self-assessment.

Step 5: Averaging and Graphic Representation

To calculate the results of the survey for each statement, all scores should be summed up and divided by the number of respondents, minus those who declined to provide their views by marking the box "Not Applicable" (N/A). A colour-code scheme is applied based on this average score. If the average score for a statement in the 7-point scale falls on the "Disagree" side of "Neither Agree nor Disagree" (below 4), it is a sign of weakness (red). If it covers "Neither Agree nor Disagree" and "Somewhat Agree" (4 and 5), then there are grounds for concern (yellow) because the status quo 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 keep up the momentum. Similarly, for the 11-point scale 0 to 4 belongs to the red segment, 5 to 7 to the yellow segment, and 8 to 10 to the green segment.

Once red, yellow, and green ratings have been assigned, the next step is to develop subgroups within each colour code or across the colour codes based on convergent or conflicting views among the respondents. Each subgroup demands special scrutiny regardless of whether they represent predominantly negative, positive, or conflicting views across the colour codes. The latter send a message that the workforce is split on an important issue of nuclear security. As evaluators identify convergent or conflicting views, tapping comments from respondents, they formulate themes to further explore with the help of qualitative data from interviews. They may also seek input from a document review or first-hand observations. Appendix IV illustrates how survey results can be graphically represented to facilitate self-assessment.

Understanding culture strengths is as important as identifying gaps and deficiencies because any effort to introduce a cultural change will be drawn both on the known strengths and deficiencies. The colour system allows for clear recognition and strong distinctions, as well as provides a basis for further

elaboration with the use of other self-assessment methods. Survey results would be easier to manage, analyse, and store if the score averaging for each statement were graphically represented as histograms. These charts aggregate the individual responses for each survey statement along with comments from respondents. See Appendix IV for more information about histograms.

General Recommendations

The designated respondents (from 40 to 50 per cent of the principal workforce) 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 as well as its rationale, procedure and 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 hour to fill out the forms. Other options for filling out the Survey Form, including electronic are possible. A major problem during a survey is to focus respondents' attention on individual statements and clarify their meaning. One way to do it is to project on the screen one statement after another providing in between enough time for selecting the appropriate box for each of them and clarifying, if appropriate, their meaning. The time required to fill out a form with 25-35 statements and several comments is estimated between 40 minute and one hour depending on the language proficiency of respondents unless the statements are translated into their mother tongue. Respondents are asked to drop their completed forms into sealed boxes to provide additional insurance of anonymity. This procedure is performed during one day at staggered hours but if respondents constitute a sizable group, this session can be extended to one or two days to accommodate their needs. Each respondent is expected to receive a thank you note from the management group for participating in the survey.

APPENDIX IV: USE OF HISTOGRAMS FOR SURVEY RESULTS

Survey results would be easier to manage, analyse, and store if the score averaging for each statement were graphically represented as histograms. These charts aggregate the individual responses for each survey statement along with comments from respondents. Figure IV–1 below is a sample of the right-skewed distribution, reflecting predominately negative views in response to a specific statement. This distribution is a clear signal that the performance quality covered by these statements is dangerously weak and measures may be needed in the follow-up action plan. 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.

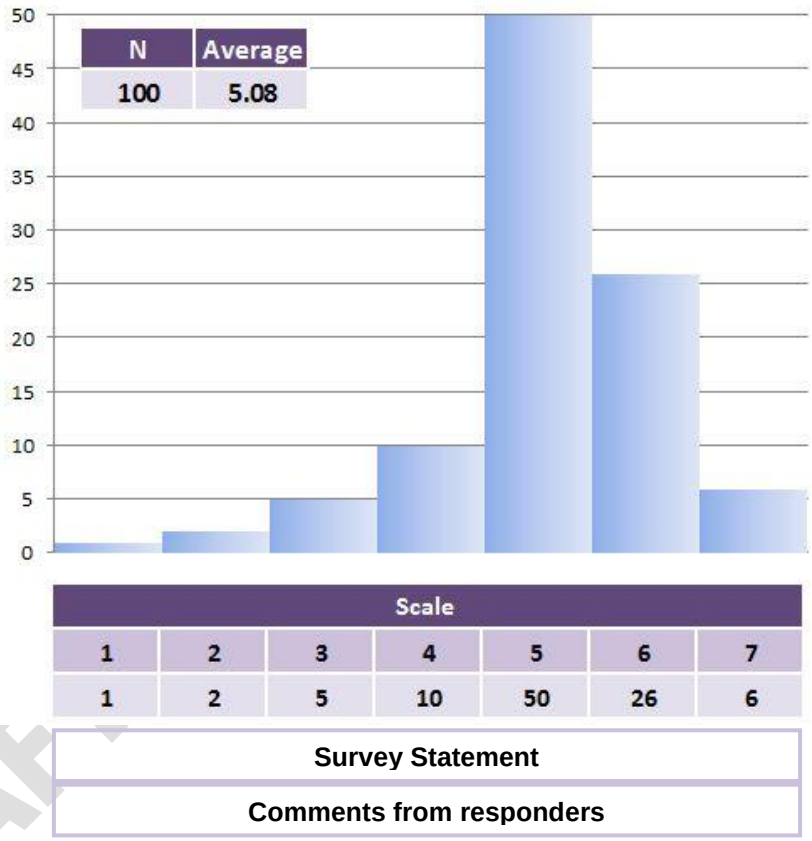

Figure IV–1. An example of post-survey graphic representation of convergent views.

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 required to develop relevant themes for interviews. A left-skewed distribution concentrating in the "Agreed" and "Strongly Agreed" section need in-depth analysis as well, because these views may represent assets that should be emphasized in the post-assessment outreach effort and to incorporated into the future action plan to overcome weaknesses and promote an effective security culture. The survey results, however, are just one step in the multi-stage self-assessment process. Even if the survey outcome is predominately positive, evaluators must not jump to conclusions because surveys

represent visible manifestations and fail to reflect deep layers of culture. Other self-assessment methods may contradict some survey results and help identify hidden problems.

Conflicting views divided between negative and positive responses are represented in what is known as bimodal or double-peaked histograms. Figure IV–2 below illustrates how these views may be distributed on the seven-point scale. Such cases warrant special attention as possible indicators of cultural flaws and must 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 evaluators may arrive is a multimodal distribution, with several peaks on both sides of "Neither Agree nor Disagree." This can signify a multi-dimensional split in the security culture fabric. The size of the "Neither Agree nor Disagree" column in Figure IV–1 is yet another symptom of the split and consistent with the overall balance of conflicting views.

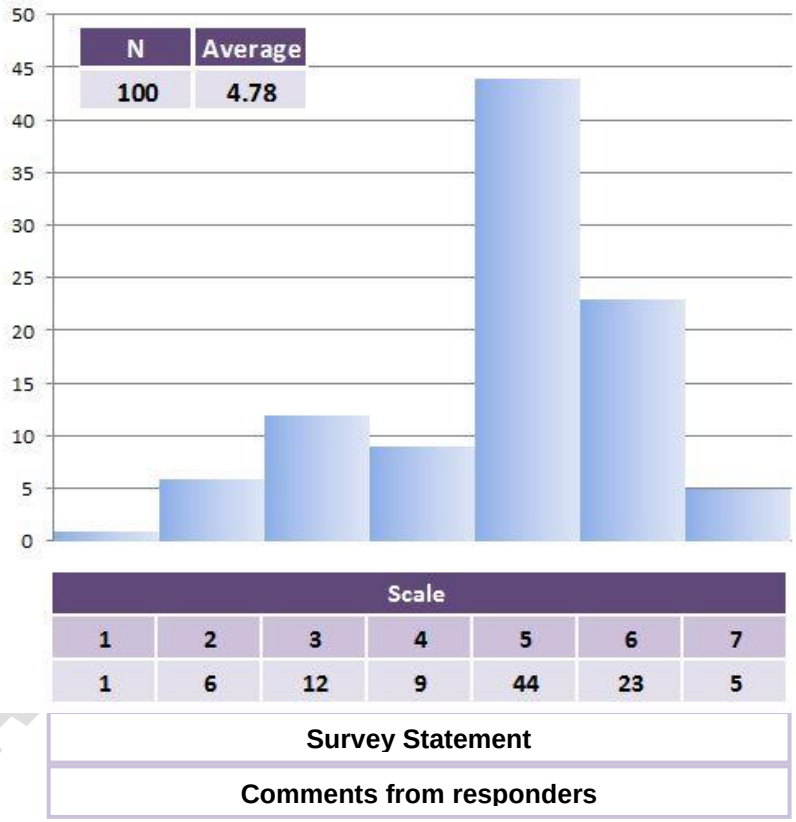

Figure IV–2. An example of post-survey graphic representation of conflicting views.

All 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 for tracking key cultural trends and avoiding human-factor risks. At the same time, plotting and interpreting histograms requires special skills from members of the self-assessment teams. They must be trained or external experts invited.

APPENDIX V: A POSSIBLE SURVEY SCENARIO

Below is a hypothetical scenario for conducting a self-assessment at a generic organization. It could be a nuclear fuel-cycle facility, a research reactor, a radioactive-sources manufacturer or user, a transport company, or any other entity under the umbrella of the assessment methodology. In our scenario, a regular audit at this organization provided evidence that the work performance of its personnel has serious deficiencies in compliance discipline. These deficiencies were identified in several units and threaten to undercut the organization's safety record.

At its regular meeting, the management team discussed the audit results and possible implications if corrective measures were not taken, 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.

A five-person self-assessment team was established by senior management and followed the step-by-step procedure recommended in the present IAEA guidance. A daunting task on its agenda was to define the topic and develop a survey as the first step in the self-assessment process. It was suggested that the key characteristic of the organization's security culture to be reinforced is "adherence to procedure," 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 should be used as survey statements, requesting respondents 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 seven-point scale ranging from "Strongly Disagree" (1) to "Strongly Agree" (7). The scheme denotes that this particular indicator presented as a survey statement is either: both fully observed and present, completely unobserved and absent, or present in part. Scoring schemes based on fewer – or more – point scale were discussed, but the seven-point scale was selected because the organization had a good experience with using it in the past surveys.

The survey also included indicators from the Management Systems and Leadership Behaviour segments 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.

The self-assessment team was cognizant that the list of indicators in Appendix II provides a set of benchmarks to illustrate how each characteristic in the Security Culture Module 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. Below is the Survey Form prepared by the Self-Assessment Team:

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 evaluation of security culture. 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 staff.

Second You are requested to evaluate the key characteristics of security culture in our 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 has partial presence and visibility. "Somewhat Disagree" and "Somewhat Agree," will give you flexibility for evaluation. Please check "Neither Agree nor Disagree" if you do not have any opinion regarding the given statement and briefly explain why. 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 don't have to identify yourself or sign it. When you complete the survey, fold it and drop it in the box located ___ (*indicate its location)* with the sign "Survey: Security Culture Self-Assessment."

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

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 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.						
If you have a comment, please leave it at the bottom of the page						

1

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
2) I am familiar with the code of conduct through ongoing training and awareness sessions.						
If you have a comment, please leave it at the bottom of the page						

2

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
3) Media-based communication systems (Intranet, newsletters, others) are used in my organization to disseminate the security policy to staff members and contractors.						
If you have a comment, please leave it at the bottom of the page						

3

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
4) Processes are in place to identify the mandatory security requirements assigned to me						
If you have a comment, please leave it at the bottom of the page						

4

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
5) Management encourages me to seek, when necessary, clarification regarding my role and responsibility for nuclear security.						
If you have a comment, please leave it at the bottom of the page						

5

6

1

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
6) I know how my security related functions fit into the broader picture at my organization						
If you have a comment, please leave it at the bottom of the page						

2

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
7) I regularly receive performance results compared with the targets. (I.(c)2)						
If you have a comment, please leave it at the bottom of the page						

3

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
8) Action is taken by the management when nuclear security performance does not fully match the goals.						
If you have a comment, please leave it at the bottom of the page						

4

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
9) I find the text of security related guides and procedures user-friendly and understandable.						
If you have a comment, please leave it at the bottom of the page						

5

6

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
10) I do not regard the procedures for all security significant activities as overburdening.						
If you have a comment, please leave it at the bottom of the page						

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
11) I was instructed during basic security awareness training on requirements for reporting security violations.						
If you have a comment, please leave it at the bottom of the page						

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
12) Systems are in place to ensure procedures and practices I learn in training are applied in practice.						
If you have a comment, please leave it at the bottom of the page						

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
13) I am aware of documented actions by senior management on negative trends in security.						
If you have a comment, please leave it at the bottom of the page						

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
14) I am aware that quality control measures are adequately enforced in the security area.						
If you have a comment, please leave it at the bottom of the page						

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
15) 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.						
If you have a comment, please leave it at the bottom of the page						

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
16) I can describe how management encourages staff members and contractors to critically review procedures and instructions during their use.						
If you have a comment, please leave it at the bottom of the page						

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
17) I can provide examples how operational performance is observed to confirm that expectations are being met.						
If you have a comment, please leave it at the bottom of the page						

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
18) Our leaders lead by example and – as is expected from all staff – by adhering to security policies and procedures in their personal conduct. (II.(a)3)						
If you have a comment, please leave it at the bottom of the page						

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
19) I witnessed how our leaders personally inspect performance in the field by conducting walk-throughs, listening to staff and observing work being conducted.						
If you have a comment, please leave it at the bottom of the page						

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
20) Managers demonstrate how their security commitments are translated into their daily job.						
If you have a comment, please leave it at the bottom of the page						

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
21) Managers spend time how to improve our security related performance coaching my team members and me at the work location.						
If you have a comment, please leave it at the bottom of the page						

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
22) I am aware of vigorous corrective and improvement action programmes that are and effectively managed. by leaders.						
If you have a comment, please leave it at the bottom of the page						

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
23) Management takes action to enforce accountable behaviour by my colleagues and me.						
If you have a comment, please leave it at the bottom of the page						

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
24) I can provide examples how management ensures that a security conscious environment prevails throughout the organization.						
If you have a comment, please leave it at the bottom of the page						

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
25) Staff members and contractors are held accountable for adherence to established policies and procedures.						
If you have a comment, please leave it at the bottom of the page						

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
26) Our organization has in place written policies, rules, or procedures for recruitment and termination of employment as they pertain to security.						
If you have a comment, please leave it at the bottom of the page						

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
27) Management regularly explains to me the importance of professionalism in the accomplishment of security tasks.						
If you have a comment, please leave it at the bottom of the page						

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
28) Leaders communicate their vision of the status of security in a variety of ways.						
If you have a comment, please leave it at the bottom of the page						

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
29) I know that there are documented definitions of responsibilities of staff members regarding security.						
If you have a comment, please leave it at the bottom of the page						

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
30) The security significance of various rules and procedures is clearly adequately explained to me.						
If you have a comment, please leave it at the bottom of the page						

1

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
31) Analysis of events or unusual occurrences consider the potential consequences arising from each incident.						
If you have a comment, please leave it at the bottom of the page						

2

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
32) It is my understanding that human factor specialists and psychologists are engaged with the organization.						
If you have a comment, please leave it at the bottom of the page						

3

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
33) Security performance indicators relevant to my work are communicated to me.						
If you have a comment, please leave it at the bottom of the page						

4

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
34) I am aware of the systems of rewards and sanctions relating to nuclear security.						
If you have a comment, please leave it at the bottom of the page						

5

6

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
35) I am aware of cases in which a security conscious attitude was a significant factor in a promotion.						
If you have a comment, please leave it at the bottom of the page						

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
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.						
If you have a comment, please leave it at the bottom of the page						

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
37) I consider myself personally responsible for security at the organization.						
If you have a comment, please leave it at the bottom of the page						

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
38) The concept of personal accountability is clearly defined in appropriate policies and procedures.						
If you have a comment, please leave it at the bottom of the page						

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
39) Procedures and processes exist to ensure clear single-point accountability before execution.						
If you have a comment, please leave it at the bottom of the page						

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
40) I recognize the importance of adhering to procedures and other protocols, such as information control.						
If you have a comment, please leave it at the bottom of the page						

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
41) Visible sanctions are applied to encourage personnel to follow procedures.						
If you have a comment, please leave it at the bottom of the page						

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
42) When I discover discrepancies in implementation of security procedures, I promptly report them to management.						
If you have a comment, please leave it at the bottom of the page						

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
43) Managers frequently inspect my work to ensure that procedures are being followed in accordance with expectations.						
If you have a comment, please leave it at the bottom of the page						

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
44) It is easy for me to follow instructions on security because they are clear and user-friendly.						
If you have a comment, please leave it at the bottom of the page						

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
45) Procedures are immediately available at my and other work stations.						
If you have a comment, please leave it at the bottom of the page						

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
46) There is a well-established practice to remind staff members and contractors through appropriate channels about the importance of following procedures.						
If you have a comment, please leave it at the bottom of the page						

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
47) Members of my team show trust in and acceptance of security procedures.						
If you have a comment, please leave it at the bottom of the page						

1

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
48) There are sufficient exchange opportunities for security relevant information within and between units.						
If you have a comment, please leave it at the bottom of the page						

2

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
49) I was involved in cross training among different professional areas and groups conducted to facilitate teamwork and cooperation.						
If you have a comment, please leave it at the bottom of the page						

3

Strongly disagree 1	Disagree 2	Somewhat disagree 3	Neither Agree Nor Disagree (Explain Why) 4	Somewhat agree 5	Agree 6	Strongly agree 7
50) My team members and I are periodically reassigned responsibility to improve inter-team communications.						
If you have a comment, please leave it at the bottom of the page						

APPENDIX VI: INTERVIEW

TABLE VI–1. ADVANTAGES AND LIMITATIONS OF INTERVIEW AS A SELF-ASSESSMENT METHOD

Interview	
Advantages	**Limitations**
• Useful for gaining insights, perceptions, and overall context	• Time consuming and labour intensive compared to other data collection methods
• Allows interviewees to focus on what is important to them	• Susceptible to interviewers' bias
• Provides new perspectives into a topic	• Requires extensive training for interviewers
• Enables one to clarify some ambiguities identified by other assessment methods	• May seem intrusive to interviewees

Semi-structured interviews can be used in the cultural-assessment process to ascertain qualitative data that surveys do not reveal—past experiences, inner perceptions, and attitudes and feelings about reality—by granting 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 make generalizations about any particular topic.

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 semi-structured interviews can be used effectively as a tool of cultural analysis. 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, the 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. 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 must be shared with all interviewers. Qualitative data relevant to the self-assessment may be derived from carefully managed discussions of:

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

Hence the development of the interview guide must 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.

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

— Look at what kind of discussion emerges when certain questions are asked and which questions need to be refined;
— 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;
— Identify new experiences shared by team members that ought to be probed at subsequent sessions;
— Identify potential interviewees based on the recommendations of invited ones.
— Reflect on the interviewer's role, preconditions, and behaviours during interviews in order to make necessary adjustments and avoid mistakes.

In the preparation stage, it is useful to put the interview guide to test by conducting a series of informal interviews. It is a format which fosters low-pressure interaction and allows respondents to see it as simply 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. Compared to the number of survey respondents, interviewees constitute a much smaller group. In determining its size and composition, the following criteria are taken into consideration:

— Those engaged must be knowledgeable about the focus of the self-assessment and willing to talk about the subject.

— As the optimal number of interviewees usually ranges from 5 to 10 per cent of the target population, inclusion of diverse professional and demographic groups is very important.
— Selected interviewees must include not just those in security and non-security fields, but administrative staff, contractors and others with expertise relevant to self-assessment.

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 an unimpeded flow of information.

An explanatory checklist must 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) An approximate length for the interview;

(e) An assurance of confidentiality;

(f) Respondents' prerogative to ask for clarification or decline to comment; and

(g) The purpose of audio or video recordings (with explicit permission).

Taking the time to explain how the interview works can go a long way towards ensuring a smooth and fruitful interview. Ultimately, it will be up to the interviewer to decide the best way to do this according to the cultural context. The interviewer must assume that there are no right or wrong answers: it is personal opinions and perspectives that are of interest to the self-assessment. Also, it is important to emphasize the voluntary nature of the interview.

Step 3: Conduct of Interviews. Interviews should be conducted in a private location with no outsiders present and where people feel their confidentiality is protected. The initial stage of the interview often exhibits elements of uneasiness and uncertainty. Therefore, breaking the ice with some general conversation beforehand helps respondents relax. Rapport with the interviewee is critical to eliciting candid and valid information. Explaining the benefits of understanding culture helps motivate interviewees, as does discussing how information obtained during the interview can help 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

identify key issues while guiding the interview along the desired path. Prompt questions should be phrased carefully to avoid steering the interviewee toward predetermined conclusions.

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 rationale behind interviews—and deepen the inquiry by encouraging participants to reflect on and reveal their true feelings. Such open-ended questions are formulated on the basis of survey analysis and can be paraphrases of indicators that were not used in the survey. Open-ended questions set no limit on the range 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?"

To catch sight of the interviewee's perceptions and experience, "***probing***" questions are frequently used during open-ended questioning. Probes are neutral questions, phrases, sounds, and even gestures 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 person appears to have more information on the subject. Excessive probing may be counterproductive. If responses are repetitive or lacking in substance, or if the interviewer becomes angered or upset about lingering on a particular topic, it is best to advance to the next question.

Probing is possibly the most important technique in interviewing, but 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.

It is important to avoid common interviewing errors:

— Asking leading questions by giving an example to make the question clearer;

- Examples offered tend to channel respondents in a direction they might not have gone without an example.
- Questions should be crafted to ensure clarity, and clarification should attempt to rephrase the question rather than supply an example.

— Rushing into pauses during the interviewee's answer;

- When there is a gap in the conversation, many interviewers are tempted to rush in with another question or a summary that puts words into the interviewee's mouth.
- Nonverbal attentiveness and body language, along with silence, encourage the interviewee to say more or go into an answer more fully. Oftentimes rich information about culture comes to light.

— Underestimating the significance of nonverbal communication.

- How the interviewer communicates nonverbally has a significant impact on the interviewee.
- Maintaining eye contact, leaning forward, and using encouraging facial expressions reinforce the impression of interest and attention, spurring conversation.

Step 4: Note Taking and Recording. Since semi-structured interviews contain open-ended questions and discussions may diverge from the interview guide, it is generally best to audio- or video-record the proceedings and, if circumstances permit, transcribe them for analysis. Whichever option is selected, it is clear that jotting notes to capture answers while trying to conduct an interview is likely to result in both poor notes and uneven rapport between interviewer and interviewee. Development of rapport and dialogue is essential in semi-structured interviews. If a respondent opts out of recording, a note-taker should be present to free up the interviewer.

Deciding when to end an interview is up to the interviewer's discretion, generally 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.

It is important to have a good data collection and management process in order to store, retrieve, and analyse the data for the ongoing and subsequent 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 debunking initial assumptions, and facilitating interpretation of the data. The end result is effective consolidation of quantitative and qualitative information.

Continuous skills improvement. The interviewer's skills have an important influence on the comprehension and complexity of the information that interviewees provide. The interviewer must be able to lend a sympathetic ear without taking on a counselling role; encourage interviewees to elaborate on their answers without expressing approval, disapproval, judgment, or bias; keep track of the questions yet let the conversation develop naturally. The core skills required to establish positive interviewer/ interviewee dynamics are rapport—building, emphasizing the interviewee's perspective, and accommodating different personalities and emotional states.

TABLE VI–2. KEY SKILLS FOR EFFECTIVE INTERVIEWING

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 one's style to suit each individual interviewee

APPENDIX VII: DOCUMENT REVIEW

TABLE VII–1. ADVANTAGES AND LIMITATIONS OF DOCUMENT REVIEW AS A SELF-ASSESSMENT METHOD

Document Review	
Advantages	**Limitations**
• Good source of background information	• Can be time consuming to collect, review, and analyse many documents
• May identify security related issues not clearly noted by other means	• Confidential nature of some documents may prevent their use in a widely circulated final report
• Unobtrusive and relatively inexpensive	• Information may be out of date
• Can provide relevant information from different time periods enabling study of tends	• May be representative of only one perspective of the issue under consideration
• Few biases about collected data	• Information in documents may not be directly relevant to the topic of self-assessment
• Information in documents is independently verifiable	

Use of document review throughout all steps of the self-assessment would serve 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:

— ***To collect background information as a general context for self-assessment***. Reviewing past and present documents helps one understand the history, philosophy, and operation of the nuclear security regime in a given organization.

— ***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.

— ***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.

— ***To acquire factual data about the issues under review***. Reviewing documents is useful for a comprehensive picture by adding, for example, the number and type of participants in security relevant events, the sequence of training sessions, etc.

Below are practical steps suggested for conducting a document review:

Step 1: Assess existing documents

Find out what types of documents exist and determine which of them can clarify specific issues

Step 2: Secure access to the documents identified as relevant to the self-assessment

Certain documents may require the permission of others or are of confidential nature. Often, senior management and legal experts need to provide authorization for access to them.

Step 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.

Step 4: Compile the documents relevant to the self-assessment

Once access is secured to the documents relevant to the self-assessment, they need to be compiled in any form available but review must be focused on the self-assessment only.

Step 5: Develop a document review protocol, checklist, or examination form

They must be systematically used by each reviewer to ensure that required information is identified, analysed, codified, and documented. Each protocol, checklist, or form includes space at the top to discuss the document and where it is stored if additional information is later required. It is useful to provide a “positive example” of a completed review protocol, check list, or examination form, highlighting how information can be recorded on the form to maximize its clarity and usability.

Step 6: Determine the accuracy of the documents

Determining the accuracy of the documents may involve comparing the 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.

Step 7: Convene reviewers' brainstorming session

When all of 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, where additional information might be found, as well as how the findings fit into the self-assessment mission.

Step 8: Summarize the information from 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 into the self-assessment process.

APPENDIX VIII: OBSERVATIONS

TABLE VIII–1. ADVANTAGES AND LIMITATIONS OF OBSERVATION AS A SELF-ASSESSMENT METHOD

Observation	
Advantages	**Limitations**
• Directly observe what people do rather than relying on what they say they do	• Only a limited number of people or events can be observed leading to a danger of generalization based on a small number of cases
• Does not rely on people's willingness to provide information	• Susceptible to observer bias
• Able to collect data where and when an event or activity is occurring	• People usually perform better when they are aware of being observed
	• Does not increase understanding of why people behave the way they do

Observations are a multi-stage process which includes the following:

— Determination of the observation object or target
— Selection of the method of results filing
— Development of an observation plan
— Selection of data processing methods
— Conduct of observations
— Interpretation of accumulated data and consolidation with other self-assessment results.

In the process of observation the focus is on:

— Physical setting
— Activities
— Human social environment (the way in which human beings interact, patterns of interactions, frequency of interactions, direction of communication patterns, decision-making patterns)
— Formal interactions
— Informal interactions and improvised activities
— Nonverbal communication

Observations typically incorporate a prescribed protocol containing specific measures of observable behaviour. Three types of data can be gathered from observations: (a) ***descriptive information***, where the

assessor notes what was actually seen (e.g., a security portal closed for maintenance during the morning peak hours, when employees come to work and walk through another gate without inspection); (b) ***inferential 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); (c) ***evaluative observations***, where the assessor both infers from and pronounces judgment on behaviour witnessed (e.g., the assessor wants to investigate whether pre-job briefings are routinely used to enhance compliance with security-related procedures. This observation assumes that pre-job 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).

Observational information comes mainly from observational notes. Effective use of observation depends on the ability to develop notes as well as 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.

Expanding observational notes involves the following:

- 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.
- 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.
- 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 must have already labelled sections to report objective observations versus interpretation and personal comments.

The observational notes include as a minimum the following:

- Location and duration of the observation.
- List of involved staff with short descriptions of responsibilities.
- List of topics (in observed meetings and discussions).
- Observed behavioural patterns, especially when related to security.
- A general estimate of the atmosphere.

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

The objective of this table is to provide select fact-based indexes that would help the management conduct observations regarding the completeness of the security management systems and their ability to function as required. They constitute a table 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.

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 of Security Management System Indexes

	a) Visible security policy	***Remarks***
	1. A nuclear security policy is established for the organization and 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 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 at the organization cover significant security items.	
	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.	

1

b) Clear roles and responsibilities		*Remarks*
	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 (design basis threat, or DBT) against which nuclear and radioactive material should be protected is determined and made known to relevant parties involved in designing, applying, and evaluating the security measures.	
c.) Performance Measurements		*Remarks*
	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 the goals.	
	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 activity and systematically motions performance	
d) Work Environment		*Remarks*
	1. Staff is consulted about the ergonomics and effectiveness of their work environment.	
	2. Top managers periodically visit manned security posts.	
	3. 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		***Remarks***
	1. A comprehensive nuclear security-training program exists, with requirements and qualification standards established and 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.	
	5. A performance-testing program is in place to ensure procedures and practices learned in training are applied in practice.	
	6. Leadership skills and best 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 best practices and lessons learned from security events.	
	12. The absentee rate during training sessions on nuclear security is low.	
	13. Staff is trained on performance testing.	
f) Work Management		***Remarks***
	1. A work plan for maintaining the integrity of the nuclear security system exists.	

	2. Contingency plans are established to address unforeseeable 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		***Remarks***
	1. Classification of documents and control requirements are defined and documented.	
	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		***Remarks***
	1. Operation and maintenance are performed according to approved procedures and vendor schedules.	
	2. Checklists/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.	
	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 performed regularly for discussing issues of mutual interest to operations and maintenance staff.	
	12. Organization has a calibration plan for security equipment such as radiation detectors, metal detectors, or other security devices requiring calibration.	
i) Determination of Staff Trustworthiness		***Remarks***
	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 like mental illness, drug/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.	
	8. The staff trustworthiness determination is periodically reviewed and updated.	
j) Quality Assurance		***Remarks***
	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 best practices for the industry.	
k) Change Management		***Remarks***
	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 which take human factors into consideration.	
	8. Before implementing changes to procedures, equipment, or organizational structure a communication process is established for staff members and contractors	
l) Feedback Process		***Remarks***
	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 to the management abnormal conditions.	
	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.	

1

	5. Discussion of pending security-related issues and changes are encouraged.	
m) Contingency Plans and Drills		***Remarks***
	1. Contingency plans are in place and are periodically exercised.	
	2. All security systems are tested periodically including systems that do not get 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 offsite 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 to increased threat.	
	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		***Remarks***
	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 best 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 best practices.	

o) Interface with the regulator (and law enforcement bodies)		*Remarks*
	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.	
p) Coordination with off-site organizations		*Remarks*
	1. Staff and management level communication with local and national organizations involved in nuclear security is regularly performed.	
	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 offsite and onsite security exercises.	
	4. 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 made.	
	7. Communication and cooperation with current and potential suppliers and contractors covers 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		*Remarks*
	1. Record keeping system for security program related information exists.	
	2. Records and logbooks are accessible to those who need them in the performance of their duties	
	3. A requirement for regular analysis of records exists.	
	4. There is a policy for protection of confidential records.	

REFERENCES

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

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Plan for 2014–2017, GOV/2013/42-GC(57)/19

[3] Amendment to the Convention on the Physical Protection of Nuclear Material, GOV/INF/2005/10-GC(49)/INF/6, IAEA, Vienna (2005).

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

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

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

[7] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Key Practical Issues in Strengthening Safety Culture, INSAG Series No. 15, Vienna, IAEA (2002).

[8] SCHEIN, E., Organizational Culture and Leadership, Fourth Edition, San Francisco, CA: Jossey-Bass (2010),

[9] SCHEIN, E., The Corporate Culture: Survival Guide, San Francisco, CA, Jossey-Bass (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 environments

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 a malicious act.

Malicious act

An act or attempt of unauthorized removal of nuclear material or sabotage.

Nuclear security culture

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

Nuclear security event

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

Nuclear security regime

The nuclear security regime comprises:

— the legislative and regulatory framework and administrative systems and measures governing the nuclear security of nuclear material, other radioactive material, associated facilities, and associated activities,

— the institutions and organizations within the State responsible for ensuring the implementation of the legislative and regulatory framework and administrative systems of nuclear security; and

— nuclear security systems and nuclear security measures at the facility level, transport level and activity level for prevention and detection of, and response to, nuclear security events.

Radioactive material

Any material designated in national law, regulation, or by a regulatory body as being subject to regulatory control because of its radioactivity.

Regulatory body

One or more authorities designated by the government of a State as having legal authority for conducting the regulatory process, including issuing authorizations.

Sabotage

Any deliberate act directed against an associated facility or an associated activity that could directly or indirectly endanger the health and safety of personnel, the public, or the environment by exposure to radiation or release of radioactive substances.

Threat

A person or group of persons with motivation, intention and capability to commit a malicious act.

Threat assessment

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