Conducting Computer Security Assessments at Nuclear Facilities

IAEA
International Atomic Energy Agency

IAEA NUCLEAR SECURITY SERIES AND RELATED PUBLICATIONS

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

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

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

Other publications on nuclear security, which do not contain IAEA guidance, are issued outside the IAEA Nuclear Security Series.

RELATED PUBLICATIONS

The IAEA also establishes standards of safety for protection of health and minimization of danger to life and property, which are issued in the **IAEA Safety Standards Series**.

The IAEA provides for the application of guidance and standards and makes available and fosters the exchange of information relating to peaceful nuclear activities and serves as an intermediary among its Member States for this purpose.

Reports on safety and protection in nuclear activities are issued as **Safety Reports**, which provide practical examples and detailed methods that can be used in support of the safety standards.

Other safety related IAEA publications are issued as **Emergency Preparedness and Response** publications, **Technical Reports** and **TECDOCs**. The IAEA also issues reports on radiological accidents, training manuals and practical manuals, and other special safety and security related publications.

The **IAEA Nuclear Energy Series** comprises informational publications to encourage and assist research on, and the development and practical application of, nuclear energy for peaceful purposes. It includes reports and guides on the status of and advances in technology, and on experience, good practices and practical examples in the areas of nuclear power, the nuclear fuel cycle, radioactive waste management and decommissioning.

CONDUCTING COMPUTER SECURITY ASSESSMENTS AT NUCLEAR FACILITIES

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

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

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

CONDUCTING COMPUTER SECURITY ASSESSMENTS AT NUCLEAR FACILITIES

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2016

COPYRIGHT NOTICE

For further information on this publication, please contact:

Information Management Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
Email: Official.Mail@iaea.org

CONDUCTING COMPUTER SECURITY ASSESSMENTS AT NUCLEAR FACILITIES

IAEA-TDL-006
ISBN 978-92-0-104616-1

Printed by the IAEA in Austria
June 2016

FOREWORD

The aim of nuclear security is to prevent, detect and respond to malicious acts that involve nuclear material, other radioactive material, or associated facilities and activities. Computers, computing systems and digital components play an increasingly important role in the management of sensitive information, nuclear safety, nuclear security, and material accountancy and control at these facilities. A compromise of computer systems could have a negative impact on nuclear security, both directly and indirectly, and could support malicious acts.

The IAEA Nuclear Security Series addresses nuclear security issues relating to the prevention and detection of, and response to, malicious acts involving nuclear material, other radioactive material or associated facilities, including theft, sabotage, unauthorized access and illegal transfer. In support of the international consensus guidance issued in the IAEA Nuclear Security Series, the IAEA also produces other publications that provide additional expert advice on specific topics.

IAEA Nuclear Security Series No. 17, Computer Security at Nuclear Facilities, sets out guidance on establishing a computer security programme at a nuclear or radiological facility. Building upon the guidance provided in IAEA Nuclear Security Series No. 17, the present publication outlines a methodology for conducting computer security assessments at nuclear facilities. Periodically performing such assessments and promptly carrying out any corrective measures is essential to the protection of computers and computing assets. The methodology described here can be applied to both internal self-assessments and external assessments. This publication is intended to be used by assessors in planning and conducting customized assessments for individual facilities and organizations.

This publication was prepared with the assistance of over thirty experts in three consultancy meetings and a number of additional expert meetings, with input from more than ten Member States.

EDITORIAL NOTE

This publication has been prepared from the original material as submitted by the contributors and has not been edited by the editorial staff of the IAEA. The views expressed remain the responsibility of the contributors and do not necessarily represent the views of the IAEA or its Member States.

Neither the IAEA nor its Member States assume any responsibility for consequences which may arise from the use of this publication. This publication does not address questions of responsibility, legal or otherwise, for acts or omissions on the part of any person.

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

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

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

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

The IAEA has no responsibility for the persistence or accuracy of URLs for external or third party Internet web sites referred to in this publication and does not guarantee that any content on such web sites is, or will remain, accurate or appropriate.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

Computer security is increasingly recognized as a key component in nuclear security. As technology advances, the use of computers and computing systems in all aspects of plant operations, including safety and security systems, is expected to increase. Nuclear Series No. 20, Objective and Essential Elements of a State's Nuclear Security Regime, stresses the importance of cybersecurity assurance activities that identify and address issues and factors that might affect the capacity to provide adequate nuclear security [1]. This is also discussed in Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) [2], which states:

> "Computer based systems used for physical protection, nuclear safety, and nuclear material accountancy and control should be protected against compromise (e.g. cyber-attack, manipulation or falsification) consistent with the threat assessment or design basis threat." (Ref. [2], paras 4.10/5.19)

A rigorous, comprehensive assessment process can assist in strengthening the effectiveness of a facility's (and State's) computer security programme. Nuclear Security Series No. 17, Computer Security at Nuclear Facilities [3], provides guidance on developing and managing such a programme. Many other publications cover information and computer security and conducting audits/assessments, such as:

- The ISO/IEC 27000 series [4–8] for information security management;
- ISO 19011:2011 [9], which provides an auditing framework;
- NIST Special Publication 800–115, Technical Guide to Information Security Testing and Assessment [10].

This publication has been written to meet the need for specific guidance for the nuclear domain that complies with international standards, International Atomic Energy Agency (IAEA) guidance, and recognized good practice.

1.2. PURPOSE

This publication outlines a methodology for conducting computer security assessments at nuclear facilities. The methodology can easily be adapted for assessments at facilities with other radioactive materials.

The guidance has been written to allow its application in multiple contexts, such as for:

- A dedicated computer security advisory service mission, organized by the IAEA at the request of a Member State;
- Computer security as a focused module within other IAEA organized missions, for example an International Physical Protection Advisory Service (IPPAS) mission where the physical protection domain is the point of evaluation;
- Assessments conducted by a national Competent Authority at sites and facilities in the State;
- Self-assessments conducted at facility or organizational level;
- A computer security assessment of vendors and third parties that provide support to nuclear facilities.

The methodology provides for the assessment of existing practices of a facility with the aim of strengthening the organization and its procedures and practices. It takes into account IAEA Nuclear Security guidance, international standards and good practice supported by the international community. It is structured as a high level review of the computer security framework, including a functional level review of the measures and procedures in place for executing that framework, with specific attention given to any nuclear security and safety functions provided by the computing systems.

Each assessment may require customization and a clear delineation of the expected outcome. For example, the expected outcome for an assessment by a competent authority (CA) may be a report on how the operator has met its regulatory and legal obligations. This report is unlikely to propose any solution paths, but it may request actions to be taken according to priorities set by the CA and follow-up assessment. In contrast, an advisory team conducting an assessment may be requested to recommend potential solutions as well as listing its findings. Advisory teams are also likely to give consideration to priorities and follow-up activities; and the scope of the assessment may specify collaboration between the assessment team and host in conducting the analysis and developing an action plan.

It is important that the objectives and expected outcomes of the assessment are clearly stated and agreed upon in the preparatory meeting.

The primary focus of this publication is to assist an assessment team in creating a customized assessment plan for an individual facility. It is not intended to be a comprehensive checklist in itself, but instead relies on the assessment team's experience in using this guidance to ensure their review is comprehensive and conducted in line with the assessment's goals and the resources allocated.

1.3. SCOPE

This publication focuses on the assessment of computer security practice at nuclear facilities of any type, including nuclear power plants, fuel cycle facilities, research reactors, etc. Although the handling of other radioactive material, transport and associated operations is not specifically covered in this publication, the principles and processes described here can readily be adapted to support the evaluation of such activities.

This publication specifically addresses only the aspects of information security that relate to computers. For example, information classification, marking, and handling requirements are not considered.

Assessment is based on reviews, interviews, and observations and normally does not include active testing of a system. In particular, the assessment detailed in this guidance does not include penetration testing or connecting test devices to the system. Members of the assessment team will not operate any piece of equipment at the assessment site, but the team may request to see active system logs or configuration files on an in-service production system. If required and within the scope of the assessment, the assessment team will request the facility to perform specific operational tasks, and active testing may be carried out as part of self-assessment or through services provided on request by an outside organization. Extreme care is needed when performing active testing on any in-service production system.

The methodology described in this publication has been written for the ideal situation: a team of three to four evaluators with 1 to 2 weeks availability on site to perform the assessment. However, consideration is also given to how the methodology could be adapted if the time and resource constraints do not support this level of effort.

1.4. STRUCTURE

This publication consists of an overview of the methodology with detailed guidance for the various stages of the assessment. It is divided into the following sections:

- Section 2 provides an overview of the assessment methodology, describing the main stages and steps that could be followed.
- Section 3 describes in more detail the preparatory activities that might be conducted in advance of an assessment.
- Section 4 details the assessment methodology.
- Section 5 provides detailed guidance on conducting the assessment, including examples of questions to ask and information to consider during the process.
- Section 6 covers activities that would typically be carried out during closure and follow-up after the assessment.
- Annex I provides hints and good practice for conducting assessments involving industrial control systems.
- Annex II provides a template for team members to collect field notes.
- Annex III provides a template for the final report.
- Annex IV lists considerations for the host organization in addressing the report results.

Figure 1 shows the basic stages of assessment planning and the projected timeline.

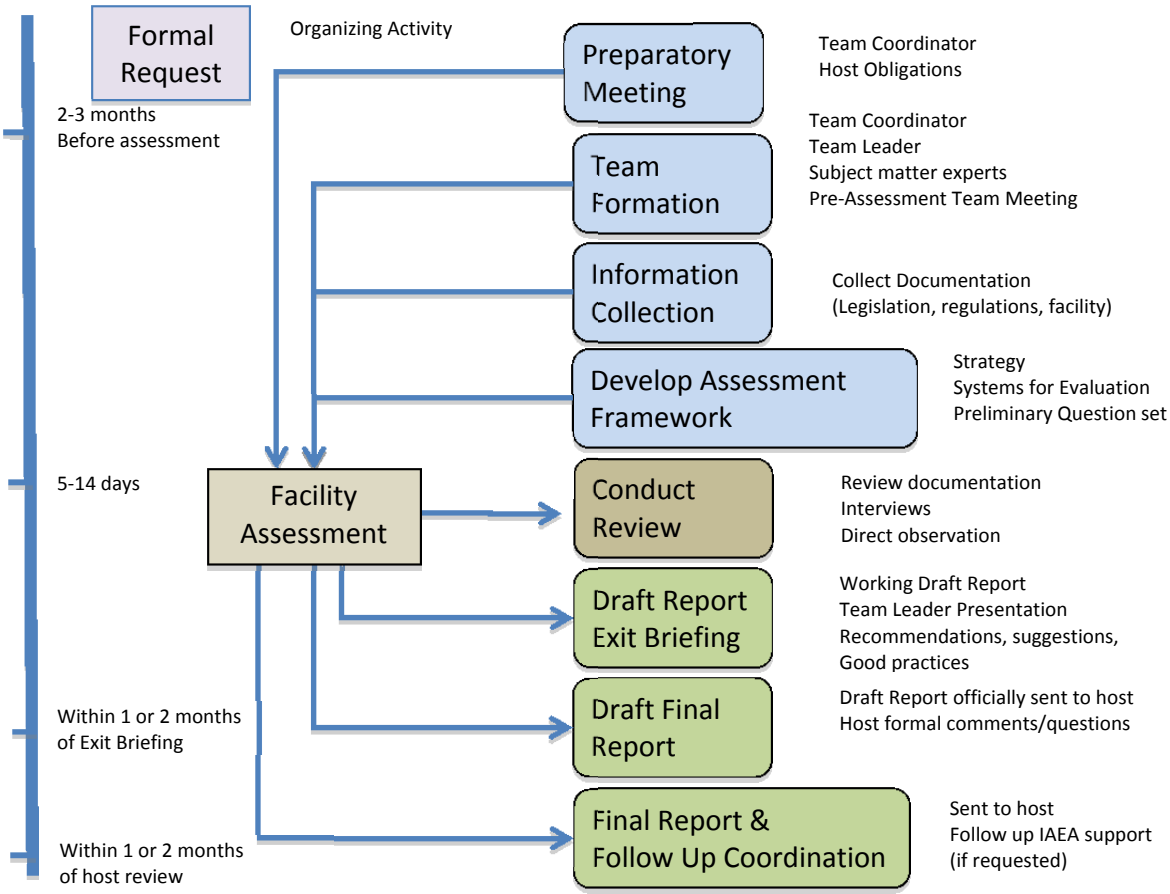

FIG. 1. Assessment steps and timeline. The timeline can be adjusted to fit resource and time constraints.

2. OVERVIEW OF THE ASSESSMENT METHODOLOGY AND PROCESS

2.1. OBJECTIVES

The objective of this assessment methodology is to help Member States and operators establish, implement, maintain and, where appropriate, strengthen their facilities' computer security, and to help their competent authorities evaluate the effectiveness of the measures taken. This publication provides high level guidance for designing and conducting an assessment at nuclear facilities or other radioactive material facilities but it is not meant to provide a comprehensive checklist for conducting the assessment. Its key purpose is to provide advice to some or all of the following:

- Facility operators on how their computer security programme can address relevant cyber threats and be structured to adapt to their evolution;
- National authorities on how to translate international recommendations into specific requirements for the State's computer security system for nuclear or other radioactive material facilities;
- Facility operators on the various methods by which international recommendations and good practice can be satisfied;
- The national competent authorities and facility operators on how to conduct an objective assessment of the status of their computer security framework and implementation of international guidance and good practice;
- Key staff of the national competent authority and facility operators, providing an opportunity to discuss their practice with experts who have experience of practice in the same field elsewhere;
- Computer security specialists from Member States, providing them with opportunities to broaden their experience and knowledge in their field of expertise.

Additionally, the assessment can be used to identify good practice that could then be communicated to other facilities and/or Member States for their long term improvement.

2.2. REGULATORY CONSIDERATIONS

This publication may be used as a reference guide for competent authorities in performing on-site computer security assessments. Additionally, the competent authority may give credit to a facility for conducting a self-assessment or may require that self-assessments are periodically conducted. The competent authority may require a site assessment to be conducted by an independent and/or third party.

The preparatory process sets out the specific standards and regulations to be used to derive the findings, recommendations and suggestions. The competent authority may request the following information as part of the assessment and final report:

- The list of findings;
- The facility's action plan for addressing the findings, including measures and timeframes;
- Evidence of a tracking system that monitors and tracks the resolution of individual findings;
- If necessary, periodic reports on the status of actions to address specific findings.

The competent authority may use these inspection results as a basis for future on-site inspections.

2.3. THE ASSESSMENT PROCESS

The elements and process flow for conducting assessment are illustrated in Fig. 2. This process will be discussed in detail.

This publication provides guidance and recommendations on how to plan an assessment and put together an assessment team. A good assessment relies on the allocation of adequate resources, a strong assessment team, and the cooperation of the facility.

Next, it provides representative assessment areas and guidance for collecting information based on the concept of functional and security domains. The assessment team creates an assessment framework — a systematic plan for evaluating the facility — in line with the planning objectives, IAEA guidance, industry standards, regulatory guides, good practice, etc. We do not provide a specific checklist for this as each assessment is unique and requires individual tailoring.

Depending on the nature of the assessment and the time constraints, the assessment team members can adjust the scope of the assessment to fit the situation and the facility's particular requirements. A comprehensive evaluation of all aspects of computer security within the scope of the assessment needs to be considered in order to make an informed judgement about the current state of the computer security programme.

When conducting an assessment, the team needs to collect sufficient information to assess the facility's computer security practices at the relevant level. The guidance provides information collection hints and recommendations on key points.

The assessment team needs to apply critical judgement in evaluating the facility's computer security framework, and its judgement based upon substantiated observations and not assumptions. The team may also make recommendations and suggestions for improvement and acknowledge good practice by the facility. It is important for the team to recognize that various approaches to the implementation of security may be acceptable (unless the competent authority has dictated a specific approach).

The product of the assessment is a final report and normally an exit briefing. As well as reporting the findings made during the assessment, the assessment report makes recommendations or suggestions that could contribute to improving the systems or processes reviewed. The report may also consider the impact of the findings on the facility's overall security and safety. It is recommended that good practice be identified and communicated to other facilities and/or Member States.

During the exit briefing, the Team Leader will present the assessment findings and, in particular, any recommendations and suggestions. It is important that the Team Leader also sets the context for the findings and any relevant related information. It is advised that the results, and especially the 'graded reports', are always presented with context and substantiation.

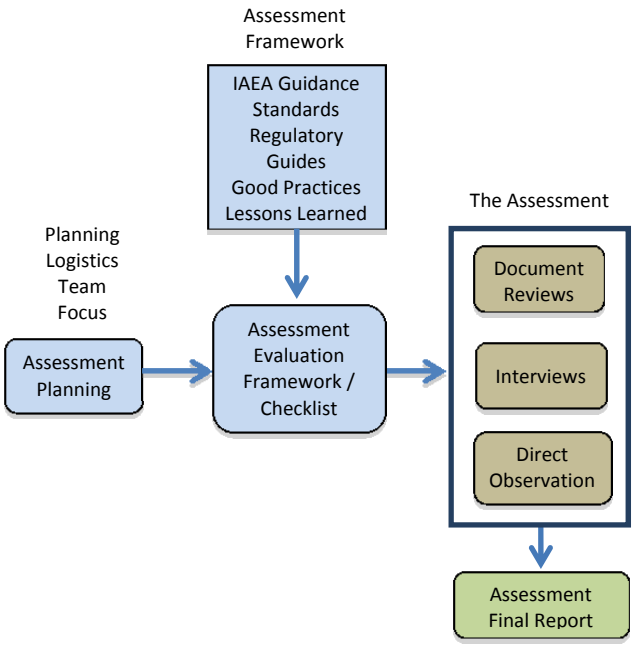

FIG.2. Assessment components.

2.4. ASSESSMENT DOMAINS

The approach to computer security assessment is comprised of two basic elements: an overall computer security programme review, and one or more system level reviews. The assessment provides a snapshot of the computer security practices at the facility. The concept presented in this publication results in a cross-domain examination of both the facility's functional operations and its computer security. This assists in ensuring coverage of processes and systems that perform primary functions, including operations, business, safety, security, and emergency response.

2.4.1. Functional domains

In general, computer systems at nuclear facilities can be mapped to one or more of the five functional domains described in this section. The assessment may be tailored to cover one or more of these functional domains (see Section 2.6 on scalability for further detail). A complete computer security assessment would cover all five domains:

i. Operations domain: computer systems used for operating the entity being assessed. These include instrumentation, control and data acquisition systems. Other systems to consider are those needed to operate the facility itself, such as heating, cooling, ventilation, lighting and elevator systems.

ii. Business domain: computer systems used in management and business oriented operation of the entity. A typical example is the work permit system. Business domain

systems typically have connections to external networks that might be relevant to other domains as well.

iii. Safety domain: computer systems that are vital for the safety of facilities and for providing protection for people and the environment against radiation risks and activities that could give rise to such risks. These include, for example, prevention and protection systems used for the shutdown of a nuclear power plant facility.

iv. Physical protection domain: computer systems used for protecting and monitoring the entity's nuclear and radiological materials. These include access control systems and physical protection systems for perimeter monitoring, and nuclear material accounting and control systems.

v. Emergency response domain: computer systems used for the detection, response and mitigation of emergency incidents which threaten public safety, health and the environment. For example, computer systems may be used in radiation and environmental monitoring, fire alarm and suppression, and emergency communications.

2.4.2. Security domains

Security domains are high level focus areas for reviewing computer security. They help provide the assessment team evaluating a functional domain with a comprehensive target for their review of the security practices. These domains are adapted from the domains described in the IEC/ISO 27002 [6]. They are:

i. Security policy;

ii. Computer security management;

iii. Asset management;

iv. Human resources security;

v. Physical protection;

vi. Communications and operations management;

vii. Computer access control;

viii. Computer systems acquisition, development and maintenance;

ix. Computer security incident management;

x. Continuity management;

xi. Compliance.

IAEA Nuclear Security Series No. 17, Computer Security for Nuclear Facilities [3] and the IEC/ISO 27000 series [4–8] together provide an initial basis for the evaluation. Industrial control system standards, good practice and lessons learned may also be considered by the assessment team when developing their assessment plan (possibly an evaluation checklist). Section 5 describes each security domain in greater detail and provides guidance for assessing each domain. Annex I provides samples of lessons learned from the evaluation of industrial control systems.

2.5. EVALUATION TECHNIQUES

An assessment team use all or some of the following techniques to acquire the information they need to develop their conclusions and recommendations:

- Review of documents and records, e.g. legislation, regulations, facility.
- Interviews with personnel from the relevant organizations such as competent authority personnel, facility operators and representatives of other organizations.
- Direct observation of the organization, its practices and systems, and the implementation of computer security measures.

2.5.1. Review of documents and records

The information collection process involves reviewing, studying or analysing facility documents and records either provided by the facility or collected there. The purpose is to:

- Evaluate the compliance of arrangements and computer security with internal procedures;
- Evaluate compliance with national laws, policies, regulatory requirements and guidance;
- Determine consistency with relevant international guidance, such as IAEA guidance, ISO/IEC standards, and good practice;
- Determine whether the arrangements and computer security measures meet established international and national good practice;
- Assess relevance to the current threat environment (e.g. the design basis threat);
- Identify processes and/or systems for detailed on-site assessment in the selected/relevant functional domains.

Documents and records may be (but are not limited to) any of the following:

- Policy;
- Procedures;
- Company forms;
- Regulatory guides/laws;
- Previous assessment reports (external, self-assessments, etc.);
- Records (e.g. training, inspection, etc.);
- Webpages (Internet and Intranet);
- Training materials (new employee orientation, computer security, etc.);
- Computer inventory lists;
- Access control lists;
- Configuration files;
- Network diagrams;
- Facility diagrams;
- Operational logs;

— Rule sets (e.g. firewalls, IDS, routers, etc.).

Section 5 lists recommended documents and records to review for each security domain, and offers hints that provide insight into specific items to look for when reviewing the documents against good practice.

2.5.2. Interviews

Interviews and discussions with individuals or groups at the facility and/or the relevant authority provide an additional level of information for the assessment. Indeed, if properly conducted these interviews are possibly the most important part of the assessment. After consideration of the relevant written material, interviews with facility personnel may be conducted to:

— Obtain additional information;

— Verify that written procedures are understood and followed as written;

— Identify assessment issues arising from previous actions or briefings;

— Elicit individual opinions;

— Form a judgement of the knowledge base, training and resources of the entity being assessed;

— Support, confirm or dispute observations made during the on-site observation of the computer security measures in place;

— Identify organization information flow and actual processes.

Interviews also provide an opportunity for important information to be exchanged between assessment team members and their counterparts in the facility. A ‘give and take’ discussion is often the best approach for an interview. An adversarial approach may not be productive. If necessary, an interpreter may be provided to avoid miscommunication. Care needs to be taken to select the appropriate personnel for the interviews to ensure the proper level of information exchange. For example, management will not necessarily be able to address technical implementation processes. Personnel recommended for interviews include (but are not limited to):

i. Management

— Head of site;

— Facility manager(s);

— Security manager;

— Safety manager;

— Information/computer/IT security manager(s);

— Head of information technology;

— HR manager;

— Emergency operations manager;

— Other management as appropriate.

ii. Technical specialists

— System administrators;

- I&C maintenance supervisor;
- System engineer (for each selected system);
- Technical operators.

iii. Other staff

- Quality assurance staff;
- Console operators.

Prior to the interview, the assessment team need to have a prepared set of initial questions or topical areas. Well-formed questions can aid in evaluating:

- Policy and procedures awareness and compliance;
- Training and security effectiveness;
- Education and security awareness;
- Threat and risks perception;
- Incident response capability;
- Clarity of roles and responsibilities;
- The effectiveness of security culture;
- Problem identification and reporting;
- Confidentiality measures;
- The application of good practice;
- The choice of technical measures and solutions to put in place.

Specifically, effective questioning can:

- Clarify questions arising from the review of the documents collected;
- Verify that personnel who are in charge of, or responsible for implementing procedures understand the security policies associated with the implementation;
- Verify that these personnel understand the implementation procedures and are properly trained and qualified to perform their job functions and/or activities.

Interviews are encouraged to be open and dynamic, leaving room for spontaneous questions and exchange of information in addition to the predefined questions.

Section 5 contains examples of questions for each security domain that the assessment team can use and adapt for their specific needs.

2.5.3. Direct observation

Direct observation of computer security measures and the implementation of procedures at a facility is an important aspect of the assessment process. A substantial part of the on-site assessment period may be devoted to observing these in practice. It is suggested that observations cover the use of procedures, site plans, instructions, regular and specific reporting and quality control measures.

On-site activities recommended for observation during assessment include (but are not limited to):

- Configuration and asset management;

— System hardening;
— Security processes;
— Physical and logical access control;
— Separation of individual duties;
— Personnel security;
— Event monitoring and logging;
— Network architecture;
— Use of good practice;
— System walk-downs/verifications.

It is also important to consider any use of compensatory controls, where one security control cannot be put in place but another is substituted instead to fulfil the same security objective. Observed activity can be compared against the facility's procedures or rules, established guidance and industry good practice. Team members' observations can then be used to judge the effectiveness of a facility's ability to implement the computer security programme.

Section 5 lists relevant activities for observation for each security domain.

2.6. SCALABILITY

The nature of the assessment may mean it is reasonable or desirable to limit the assessment to certain functional areas covered in this guide. The guidance in this publication is flexible and may be scaled in line with different approaches and time frames depending on the assessment level.

2.7. INFORMATION SECURITY CONSIDERATIONS

The assessment will examine sensitive information and sensitive information assets. Reports and working documents may contain sensitive information, unauthorized disclosure of which could compromise nuclear security and lead to severe consequences. It is therefore imperative that preparatory material, technical notes, draft reports and the final report are appropriately classified, marked, handled, stored, transmitted and destroyed in accordance with the relevant procedures for sensitive information at the host facility. The handling and security of such information need to be discussed during the Preparatory Meeting and determined prior to the assessment.

Team members circulating their technical notes to other team members for comment must take special precautions to ensure the security of sensitive information. Consideration also needs to be given before the assessment to the types of electronic devices or storage media that will be used for individual note-taking and the compilation of draft and final reports.

It is recommended that the security of this material be based on the 'need to know' principle, i.e. access to the material is restricted to individuals whose trustworthiness and need to know have been established.

Depending on the context of the assessment, it may be necessary for the assessment team members to sign a confidentiality or non-disclosure agreement.

3. PREPARATORY ACTIVITIES

3.1. SCOPE OF THE REVIEW

Given the number of computer systems in nuclear facilities and the breadth of the functional and security domains to assess, it may be impossible to conduct a comprehensive review of the entire computer security programme within a single assessment. The first step is therefore for the host to decide the scope and objectives of the assessment and to explain these to the Team Coordinator or Team Leader as appropriate. Section 4 presents the concept of modular components for specific facility functional domains. This approach allows the assessment planners to identify priority components for a tailored assessment.

3.2. PREPARATORY MEETING

The preparatory meeting, involving the Team Coordinator and Team Leader, is usually held around two to three months prior to the assessment and at the host facility to allow representatives from all the parties involved to participate. The desired outcome of this meeting is a clear understanding of the assessment process and methodology including preparation activities, the mechanics for conducting the assessment, and the post-assessment reporting activities. A record of the meeting may be circulated.

The meeting will consider:

- The main features of the assessment programme;
- The objective and scope of the assessment;
- The expected format and contents of the report;
- The scope and level of analysis to be included in the report;
- Information handling and security requirements for the report and technical notes;
- Preparation for the assessment, including a list of the documents required;
- Preparation of an advance information pack for the assessment team;
- The logistical support required, such as the team office, printer, copier, and local transportation;
- Provision of translation/interpretation services;
- The handling of confidential documents from the subject facility;
- Procedures for the assessment team to follow — including the immediate actions to be taken and the point of contact within the host organization to be notified — if any of the following events are identified:
    - An actual or potential system compromise,
    - Wilful negligence,
    - A major safety issue,
    - A major security issue;
- Finalization of the assessment schedule;
- Potential composition of the assessment team members;
- Possible follow-up activities.

3.3. HOST OBLIGATIONS

The host is considered to be the sponsor of the activity. The host may consist of facility management or a government agency for a facility review, or a government agency, if the assessment activity centres on a State level review. As part of the discussions at the preparatory meeting, the Team Coordinator and Team Leader will make arrangements with the host to ensure the provision of the support facilities needed at the assessment location. For an international mission, computer security assessments are usually conducted in English. The host needs to provide any necessary interpretation to allow team members to do their work.

It is important that the host provide the assessment team with exclusive use of a secure meeting area for the entire period of the assessment. This secure meeting area needs to be of sufficient size to enable the team to work and to hold discussions in reasonable privacy. Internet access may also be desired, but needs to be discussed in the initial preparatory meeting. A computer printer and a copying machine are recommended to be made available to team members. Relevant documents to be discussed at the preparatory meeting are to be supplied in a language agreed between the host and the assessment team. A container, or an area with additional physical protection measures in place, to provide for the secure storage of documents or assets that may contain confidential or sensitive information is required by the assessment team during the assessment period.

To save time during the assessment and allow the team members to obtain a good understanding of the context of the assessment and the regulatory requirements, it is desirable that the host provide relevant documents for circulation to the team members at least two months prior to the team's visit, recognizing that some documents may not be readily available until arrival at the facility. All documents obtained from the host need to be handled in accordance with the agreement between the host and the team.

Depending on the scope of the assessment, these documents could include:

i. National legislation:
   - Law(s) governing the computer security of nuclear facilities; a synopsis of the responsibilities and structure (specifying relevant departments) of the various government organizations that deal with computer security issues and how they interrelate;
   - Regulations on the computer security of nuclear facilities;
   - Relevant regulatory guidance on nuclear facilities;
   - Design Basis Threat characteristics.

ii. Regulatory authorities' organizations and procedures:
   - Structure, organization and staffing; a description of the licensing procedures where applicable;
   - Inspection practices;
   - A list of applicable regulations, regulatory guides, codes and standards.

iii. Facility description, organization and computer security procedures:
   - Overall security policy (or relevant sections of this);
   - Computer security plans;
   - Security roles and responsibilities;

— Security training and awareness programme;
— Inventory of digital assets and a description of how and why the digital assets are within the scope of facility's computer security programme;
— Third-party involvement;
— Risk assessment, including a description of how security controls are selected;
— Safety system categorization;
— Safety procedures relevant to security;
— Network architecture design;
— Boundary devices between network domains, including data flow policies for the devices;
— System technical documentation;
— Existing assessment reports (prepared by the facility itself or a third party);
— Computer security incident response procedures and records;
— Computer security incident reports and corrective measures;
— Configuration management documents including security analyses associated with the configuration changes.

3.4. TEAM FORMATION

3.4.1. Team composition

The team may be comprised of a Team Coordinator, a Team Leader (where appropriate), three or more experts and, possibly a technical writer to assist the team in developing technical notes and the final assessment report. The composition of the team may be adapted according to the scope of the assessment.

The Team Coordinator or the Team Leader selects experts for the team, with the agreement of the host. These experts need recognized broad knowledge and extensive experience in computer security, as well as specialization in one or more areas of plant operations, safety, physical security, facility information technology and engineering to support the evaluation of the Functional Domains. Team members need to be able to commit to a specific period of time for preparation, the assessment itself, and final reporting. It helps the assessment if at least one team member is familiar with the design of the facilities operated by the host.

In addition, it is recommended that team members are selected so as to reflect different national approaches to regulation and implementation, such as relevant legislation, regulation of nuclear activities, operation of facilities, and analysis of computer security systems. Each of the experts, in addition to their particular area of expertise, is likely to have knowledge of other national approaches and other relevant areas. As a result, the team will be able to provide the best possible computer security assessment and advice.

An observer from the host may be invited to participate in the assessment with the team. This can prove beneficial in facilitating the exchange of information.

3.4.2. Team Coordinator

The Team Coordinator will accompany the team throughout the assessment to coordinate with counterparts in the host organization and to provide any logistical and other support that may be required. In the case of an IAEA advisory service mission, the Team Coordinator will circulate the current edition of relevant assessment documents and any other material that may be applicable, in addition to the advance material provided by the host country, to all team members so that they can become familiar with the documents they will be using throughout the mission.

The Team Coordinator has overall responsibility for coordinating the assessment and delivering the final assessment report.

Responsibilities include:

- Coordinating the preparatory work and making the necessary arrangements for the assessment;
- Establishing liaison contacts with appropriate host organization counterparts who will be the primary contacts for the assessment team during the mission;
- Designating, in conjunction with the host organization if appropriate, a computer security expert to be the Team Leader for the assessment;
- Arranging, in conjunction with the Team Leader, for a preparatory meeting with the host;
- Selecting, with the approval of the host organization, the team members;
- Coordinating logistical arrangements in support of the assessment team, including the supply of relevant briefing documents;
- Being aware of the relevant rules of the facility regarding safety, security, personnel safety, and any other applicable requirements, and communicating this information to the assessment team.

3.4.3. Team Leader

The Team Leader is particularly important for the success of the assessment. Individuals selected as Team Leaders must have recognized leadership qualities and very broad experience across the full scope of review activities that are likely to confront an assessment team. The Team Leader will ideally have experience of conducting computer security assessments in nuclear facilities.

The Team Leader typically has overall responsibility for:

- Representing the team in interactions with his or her counterpart in the host organization;
- Leading the preparatory, entry and exit briefing meetings;
- Determining the rules of engagement for all team members;
- Briefing team members on the assessment including its objectives and processes;
- Ensuring that team members have the necessary information to be properly prepared for the assessment;
- Leading development of the detailed assessment activities and schedules;

— Coordinating and supervising the team's review activities, including conducting daily team meetings, ensuring that schedules are met, keeping his or her counterpart informed, resolving issues that require decisions, and preparing for the exit meeting;

— Coordinating the review of all the technical notes;

— Coordinating the production of the draft report;

— Presenting the assessment results at the exit briefing;

— Producing the final report;

— Ensuring that team members are aware of confidentiality issues and handle information accordingly;

— Ensuring that team members are aware of and trained in any relevant rules for the facility regarding safety, security, personnel safety, and other applicable requirements.

3.4.4. Team members

Team members will conduct the assessment, gathering information, evaluating, and providing input to the final report. They will have computer security expertise and additional expertise in the operation of the organization or facility.

Team member responsibilities and duties include:

— Conducting document and record reviews;

— Participating in meetings and discussions with their counterparts in the host organization as appropriate;

— Attending team meetings and participating in the development of assessment activities;

— Comparing conclusions/findings with other team members;

— Developing technical notes on the implementation of computer security measures at the host facilities based on presentations, documentation, interviews, and direct observation of the organization and its practices;

— Evaluating systems within the functional domains against security domain controls;

— Remaining aware of the confidentiality agreement with the organization and handling all information accordingly;

— Being aware of, and complying with, the relevant rules of the facility regarding safety, security, personnel safety, and other applicable requirements.

3.4.5. Technical writer

A technical writer may be beneficial for the team in supporting the timely completion of the assessment report and assisting individual team members in the development of technical notes. The technical writer attends all meetings, briefings and interviews to take notes to supplement the information gathered by the team. Throughout the assessment, the technical writer collects written input from the team and formats and edits the material as appropriate. Responsibilities and duties include:

— Participating in team activities;

— Taking extensive notes and/or assisting team members in preparing for observation and interview activities;

— Together with the team and team leader, developing the assessment report;
— Remaining aware of the confidentiality agreement with the host organization and handling all information accordingly;
— Being aware of and complying with the relevant rules of the facility regarding safety, security, personnel safety, and other applicable requirements.

3.5. PRE-ASSESSMENT TEAM MEETING

It is recommended to have a team meeting prior to the commencement of the assessment in order to ensure coordination among the team. This is particularly important if the team has not previously worked together, as would be the case with international missions with experts from different countries. Even if the team work together regularly, it can still be advantageous to have a pre-assessment meeting to discuss and clarify the specific details of this particular assessment.

Depending on the nature of the mission or assessment, this meeting might be organized several months in advance, or immediately prior to the commencement of the assessment.

The meeting is run by the Team Coordinator and Team Leader. Agenda items might include:

i. Introducing the team members;
ii. Assessment background:
    (a) Scope of the assessment;
    (b) Schedule and timeframe for assessment activities;
iii. Team members' background:
    (a) Skill and knowledge of the team members;
    (b) Expectations of team members;
iv. Discussion of factors unique to the assessment and the nuclear facilities to be visited;
v. Discussion of the detailed assessment process;
vi. Development of detailed roles, responsibilities and areas of focus for each of the team members.

3.6. SCHEDULE OF THE ASSESSMENT

The schedule of the assessment will depend greatly on whether it takes place at one site or many, is a dedicated assessment, or a module within another assessment, mission, or advisory service. Table 1 suggests a notional schedule for a dedicated computer security assessment, in which most days will be spent on site, and a technical writer updates a draft report daily.

TABLE 1. NOTIONAL ASSESSMENT SCHEDULE

Day 1
Assessment team meet for pre-assessment team meeting and orientation session
Day 2
Team receive the necessary training to enter the host facility
Entry meeting with the host facility
Begin assessment
Debriefing meeting and preparation for the next day
Technical writer prepares daily report from the debriefing
Team Leader briefs a manager who represents the host organization as necessary
Day 3 to Final Day-2
Begin assessment
Debriefing meeting and preparation for the next day
Technical writer prepares daily report from the debriefing and compiles the collected daily notes and reports
Team Leader briefs a manager who represents the host organization as necessary
Final Day-1
Team members discuss and summarize the assessment
Technical writer drafts an exit report for the team members' review
Team Leader develops a presentation for the exit briefing
Team Leader briefs a manager who represents the host organization as necessary
Final Day
Exit briefing — briefing of the host organization on the result of the assessment

3.6.1. Team meetings

Daily team meetings, typically held at the end of the day, are useful to review the day's activities, evaluate progress, discuss findings/conclusions developed by team members and ensure the technical writer has the required information from the day's activities.

This meeting can also be used to prepare for the next day's activities, for example by:

- Reviewing appropriate areas of the assessment guidelines and/or preparatory material;
- Making a list of questions on each topic;
- Planning field observation activities;
- Identifying the main issues to prioritize for the next day.

4. ASSESSMENT METHODOLOGY

4.1. OVERVIEW OF METHODOLOGY

A typical start to an assessment is to evaluate the computer security practices of the facility from an overall perspective. Then, a more detailed analysis can be made on selected processes and systems in line with the approach described in Section 4.3.1. This is based on dividing the computer security practices into functional and security domains. This process will help refine the evaluation of the effectiveness and quality of the whole computer security programme.

4.2. ASSESSMENT OF THE OVERALL COMPUTER SECURITY PROGRAMME

At the information collection stage, the assessment of the overall security programme involves a review of relevant policies, plans, procedures, implementation and organization charts. Interviews and field observations will help in further evaluating computer security practices. Four aspects that make up the overall view to be considered are: the management approach, computer security processes, threat and consequence management, and risk management.

The following sections provide indicative criteria for each of these aspects on which the assessment could be based.

4.2.1. Management approach

One of the key elements of a successful computer security programme is acceptance of the computer security policy at all levels of management and operations and its implementation in practice. The computer security programme will not succeed without strong management commitment to the process. Indicative criteria include:

i. Management commitment is demonstrated at all levels.

ii. Computer security objectives are clearly defined.

iii. Clear roles and responsibilities have been established to ensure that computer security processes, including specific roles and responsibilities:

   (a) Extend across all functional domains;
   (b) Are established with a coordinated approach between relevant functional domains;
   (c) Provide adequate organization (including a dedicated Computer Security Officer or equivalent).

iv. Management provides access to adequate resources (human, financial, time allocation, skills, etc.).

v. Management processes include internal assessment and quality assurance measures.

vi. Compliance with the regulatory framework is ensured.

4.2.2. Computer security processes

This refers to the use and application of computer security measures in the implementation of the computer security policy. This includes the application of technical controls, administrative control, and physical controls to prevent, detect, and respond to computer security events. Indicative criteria include:

— A computer security policy and a computer security programme exist;

— There is a structured, formalized, documented set of processes that address computer security;

— Processes in place allow continuous review and improvement, e.g. periodic reviews, audits, clear maintenance procedures, self-assessments, etc;

— Processes are proactive to the greatest degree possible and not reactive.

4.2.3. Threat and consequence management

Using credible information sources, the appropriate State authorities — and facilities as appropriate — define the threat and associated capabilities in the form of a threat assessment and, if appropriate, a design basis threat. Threat considerations include analyses of adversaries with a credible cyber capability. It is advised that the threat be continuously reviewed and evaluated for indications of any changes that might affect the computer security of the organization or facility. Indicative criteria and questions include:

— The organization has a mature management process in place that addresses threats, vulnerabilities and potential consequences.

— Which references and methodology are used?

— What is the scope of the threat analysis (e.g. the organization, part of the organization, a system, etc.)?

— How the analysis was performed, documented, and used in conjunction with baseline security controls.

— Potential targets have been identified and assessed to determine if they require protection from nuclear security threats.

— Assessments include an analysis of the potential consequences associated with cyber-attacks against the targets.

— With regard to the manner in which threat evaluations are conducted, how frequent are regular reviews and updates?

— Are mitigation, continuity and recovery processes that have been defined for computer compromise supported within the incident response programme?

4.2.4. Risk management and adherence to fundamental security principles

The State and facility need to ensure that the computer security programme is capable of establishing and maintaining the risk of computer compromise at an acceptable level through risk management. The computer security programme needs, additionally, to detail the application of fundamental security principles, including the use of a graded approach and defence in depth, to protect assets against nuclear security events according to the level of consequence or impact those events might cause. Indicative criteria and questions include:

— Computer security measures are based on a graded approach. In particular, security levels have been assigned in line with clear processes or rules (e.g. based on safety, the design basis threat, potential consequence analysis, etc.). Are these processes or rules actually being applied?

— How is defence in depth implemented for computer components and systems?

— How do risk assessments influence the graded approach?

— Does the graded approach address all items identified by the risk assessment?

4.3. ASSESSMENT MATRIX

4.3.1. Introduction

A core element of this assessment methodology is an evaluation of functional domains and security domains (introduced in Section 2.4). Table 2 provides a matrix designed to identify both types of domain for evaluation, ensuring that the assessment covers the areas of direct interest in sufficient depth. The assessment matrix contains:

— The five main functional domains as columns;

— Security domains (adapted from the domains found within the ISO 27000 series) as rows.

This matrix is intended to provide support with:

— Identifying the scope of the assessment;

— Structuring the outcomes of the analyses and observations, both at the information collection stage and in the field;

— Helping to give the assessment team a sufficiently broad analysis with which to make an informed evaluation;

— Visualizing the results of the assessment.

4.3.2. Functional domains

A global assessment involves an evaluation of the five functional domains: operations, business, safety, physical protection and emergency response. In some cases, a more limited scope that focuses on a subset of these domains is possible (e.g. in a typical IPPAS mission, only the physical protection would be evaluated).

An indicative list of families of systems or functions for evaluation is provided below for each of the five functional domains. This list will vary and can be tailored to the individual facility to be evaluated. It may also be adapted in line with the scope of the assessment and the type of facility. This selection may change during the assessment, if necessary, to capture additional elements encountered during the on-site activities. Examples of systems or functions within each domain include:

Operations domain

— Process control systems: instrumentation and control (I&C) systems for plant control;

— Control room I&C including the alarm systems;

— Process computer systems that collect and prepare information for the control room;

— Fuel handling and storage I&C systems;

— Configuration management/maintenance;

— Remote access and virtual private networking (VPN) for the operational environment;

— Voice and data communication infrastructure;

— Infrastructure operating and control systems;

— Test and development environments for operations systems.

Business domain

— Voice and data communication infrastructure;

— Human Resource Management systems and data repositories;

— Technical/engineering systems;

— Work order and work permit systems;

— Procurement systems;

— Office systems.

Safety domain

— Protection systems: I&C systems used for automatically initiated reactor and plant protection actions;

— Safety actuation systems: I&C systems that perform safety actions, initiated by the protection systems and by manual actuation;

— Safety system support features: I&C for emergency power supply systems.

Physical protection domain

— Perimeter monitoring/ intrusion detection;

— Access control systems;

— Accountancy and Inventory Control systems (other than for nuclear materials);

— Nuclear material accountancy and control systems;

— Voice and data communication infrastructure;

— Alarm systems;

— Security clearance database, used to ensure that personnel hold the appropriate security.

Emergency response domain

— Environmental monitoring;

— Radiation monitoring;

— Fire protection systems;

— Voice and data communication infrastructure.

The final report will identify which systems and functions were evaluated and which systems and functions were considered outside the scope.

4.3.3. Security domains

In contrast to the functional domains, the assessment may address the complete set of eleven security domains in order to ensure sufficiently broad coverage for the review. As stated earlier, the eleven security domains are adapted from the ISO/IEC 27000 series [4–8]. They have been customized for use in computer security assessments at nuclear facilities. Section 5 provides specific guidance for evaluating each of these domains with regard to nuclear security. This is indicative and not a prescriptive list.

Table 2 provides a cross matrix of the security and functional domains, which may be used to track the coverage of the assessment and ensure a comprehensive review of the desired areas. Use of such a matrix is at the discretion of the assessment team. In addition to verifying assessment coverage, the matrix may assist in visualizing observations across different domains, which may help to identify trends or gaps in security coverage.

TABLE 2. DOMAIN COVERAGE MATRIX.

Functional Domains **Security Domains**	**Operations**	**Business**	**Safety**	**Physical Protection**	**Emergency Response**
Security Policy					
Computer Security Management					
Asset Management					
Human Resources Security					
Physical Protection					
Communications and Operations Management					
Access Control					
Acquisition, Development and Maintenance					
Computer Security Incident Management					
Continuity Management					
Compliance					

5. ASSESSMENT GUIDANCE BY SECURITY DOMAIN

5.1. OVERVIEW

This section provides guidance and good practice related to each of the eleven security domains to use as potential evaluation criteria during the assessment. This guidance is not designed to be used directly as a checklist, but may be used to create a tailored assessment plan. Team members need to pay attention during the assessment not only to the individual domains, but also to their integration and their impact on the overall computer security programme.

5.2. SECURITY POLICY

5.2.1. Security domain description

This domain provides management direction and support for computer security in accordance with nuclear safety and security, as well as relevant laws, regulations and business requirements.

Management needs to set a clear policy direction in line with nuclear safety and security, and demonstrate its support for, and commitment to, computer security by establishing and maintaining a computer security policy across the organization.

The computer security policy is to be defined, communicated, documented and periodically reviewed. It is recommended that the policy take into account all five nuclear functional domains: operation, business, safety, physical protection and emergency response.

Documents and records of interest

- Computer security policy/plan;
- Facility physical security policy/plan;
- Computer security policy communication to employees;
- Record of computer security audits;
- Record of security policy review and updates;
- Records of computer security exercises.

Documents and records analysis hints

- Has the security policy been defined?
- Is the policy consistent with other facility policies?
- How is the security policy communicated to employees?
- How is management commitment demonstrated?
- How often is the policy reviewed for changes? Is there a record of this review?
- How does management evaluate the effectiveness of the policy?
- Does the security policy address all five nuclear functional domains?
- If exceptions to the security policy exist, are these documented?

— Is the security policy communicated to third parties (subcontractors, etc.)?

— Does the policy address current good practice guidance?

— Does the policy clearly state the security objectives?

— Are responsibilities clearly defined, and the corresponding authority assigned?

Sample interview questions

— Are they aware of the security policy?

— Do they understand the roles and responsibilities (including their own)?

— Do they have access to the security policy?

— How is the security policy implemented in specific guides or instructions relevant to their work?

Items to observe

— Specific processes relevant to policy implementation;

— When relevant, check consistency between policies.

Field analysis hints

— Ask the same questions to people from different departments and at different levels in the organization.

5.3. COMPUTER SECURITY MANAGEMENT

Security domain description

A management framework for computer security needs to be established within the organization.

Management needs to approve the computer security policy, assign roles and responsibilities, and review the implementation of computer security across the organization. This may actually be a component of a larger security policy. A multi-disciplinary approach is encouraged across all organizational departments (e.g. IT and I&C/Engineering).

Documents and records of interest

— Computer security policy/plan;

— Organization charts and job descriptions;

— Policy and procedures detailing the organizational structure;

— List of Computer Security Officer(s) and computer security team members;

— Description of the authorization process for computer security policy/procedure modifications;

— Procedure and authorization process for procuring new information processing equipment;

— Training programme, policy and records.

Documents and records analysis hints

- What are the computer security objectives?
- Where in the organizational hierarchy do the computer security responsibilities lie?
- What is the structure of the computer security team?
- All functional domains are covered by a computer security officer (CSO). If there is more than one CSO, responsibilities and lines of communication need to be clearly defined. Clearly defined interfaces with roles and responsibilities are required.
- Do the modification procedures include computer security?
- Is there specialist training for those with security functions?
- Who is required to be trained, how often are they trained, and what percentage of staff have received the required training?

Sample interview questions

- Do you know who your Computer Security Officer is and how to contact him/her?
- What are the baseline computer security procedures?
- Does the computer security team hold regular meetings? Are minutes taken of the meetings? What is the process for notifying the computer security team of events and incidents or changes that could compromise security?
- What is the process (i.e. the tools or procedures) for protecting sensitive information?
- What computer security training have people had? Is this continuous?
- Has a skills analysis been performed on the existing internal organization to identify any skills gaps? How have these gaps been addressed?

Items to observe

- Do the computer security specialists have relevant external training on computer security?
- How are computer security tasks tracked and followed up (e.g. through action points from minutes of the meetings)?
- Is there an assigned person for computer security audits/assessments? Are audits/assessments incorporated into the yearly planning?

Field analysis hints

- Members of computer security team are advised to be involved in the assessment.
- Is computer security visible at all levels of management and staff?

5.4. ASSET MANAGEMENT

Security domain description

The goal of this domain is to protect organizational assets. It includes responsibility for asset management, an inventory of authorized hardware and software, a list of unauthorized

hardware and software, and computer classification (of systems important for safety and/or security).

All assets need to have a dedicated owner who is responsible for assigning appropriate controls.

Documents and records of interest

- Policy and procedures detailing the asset management system;
- Inventory of assets (computer systems, network equipment, software, version);
- Procedures and criteria for identifying computers within the scope of the computer security programme, if applicable;
- Listing/diagram of the physical location of inventoried assets;
- Inventory procedures, including periodicity and records of inventory updates;
- Functional diagram of systems and associated computer assets;
- Zone model diagram (if applicable);
- Policy and procedure for classifying sensitive information.

Documents and records analysis hints

- Asset management covers the full asset lifecycle;
- Which part of the organization made the inventory?
- Who maintains the inventory?
- Who has access to it?
- Traceability of changes;
- Protection of the inventory (including backups);
- How is asset classification conducted? Is it documented? What is the quality?
- Are assets assigned to a zone and managed with regard to a 'zone model'?
- Are 'security levels' defined? What are the security measures taken for each level?
- Are security levels assigned to specific zones? What is the basis for such assignment?
- Does the physical location match the inventory?
- How does the zone model compare to the physical location of a system?
- How are assets labelled in accordance with the classification by functional domain?
- How does the classification translate into logical zones (cf. the graded approach)?
- Check if the equipment is connected to more than one zone;
- Have the physical protection measures been assessed in terms of computer security?
- What reliance do the physical protection measures have on the computer and/or networking systems?

Sample interview questions

- What are the security measures for the observed level?

— Do you have or can you access, the asset inventory list?

— Are external or private devices allowed, and under what circumstances? (Ask about the security controls in place)

— How are lifetime issues resolved (how new equipment is chosen and maintained and what the retirement process is)?

— How is third-party owned equipment handled?

Items to observe

— Verify specific devices against the network diagram.

— Is this computer connected to the appropriate network?

— Is the device correctly labelled in accordance with policy?

— Are the security measures implemented for this asset?

— Check the consistency between the inventory and equipment in the field (e.g. random verification).

— Check the version management as well as parameter configuration management.

— How is the confidentiality of assets and inventory managed?

— From where and how are the administration and maintenance of network attached assets carried out?

Field analysis hints

— Does the physical location match the inventory?

— Does the zone model match the physical location of a system (or part of it)?

— How are assets labelled in accordance with the classification by functional domain?

— How does the classification translate into logical zones or security levels (cf. the graded approach)?

— Check if the equipment is connected to more than one zone.

5.5. HUMAN RESOURCES SECURITY

Security domain description

The objective is to ensure that employees, contractors and third-party users — i.e. all personnel with responsibilities within the organization — understand their roles and responsibilities for computer use and for computer security. Security responsibilities need to be addressed prior to employment as terms of employment and throughout the employment or contract of the individual.

Trustworthiness evaluation (also called personnel vetting) is advised for all candidates for employment, contractors and third-party users as appropriate to their level of access to sensitive data and systems. Employees, contractors and third-party users of information processing facilities are also encouraged to sign an agreement about their security roles and responsibilities and participate in training programmes appropriate to their responsibilities. This may be subject to relevant national laws, which need to be taken into consideration.

The computer security awareness-building programme is an ongoing process promoted by management.

Documents and records of interest

- Policy and procedures regarding computer use and security for employees, contractors and subcontractors;
- Records reflecting personnel management for computer use and security;
- What measures are taken to control the consistency between privileges and employee status (access rights management according to role)?
- Policy and procedure for personnel training (orientation, by function, refresher training);
- Certification/qualification records and job placement requirements for computer security team individuals.

Documents and records analysis hints

- How often do personnel undergo computer security awareness training?
- What is the procedure for getting access to computers, applications and data?
- What is the process for getting access to sensitive data and applications?
- How is the computer security culture assessed for effectiveness?
- Do you publish a staff directory online? In what format, with what information?
- What is the company policy on the use of social media?
- Which personnel require trustworthiness checks?
- What is the consequence if someone violates security procedures?
- Are penalties adequate and correctly applied? Is good behaviour appropriately rewarded?
- Is a 'Notice of Use Agreement' or 'Technology Acceptable Use Policy' defined? This may be implemented as a splash screen on computer account login.
- Do computers, where appropriate, have a password protected screen saver? What is the time delay?

Sample interview questions

- How often do personnel undergo computer security awareness training?
- What is the procedure for getting access to computers, applications and data?
- What is the process for getting access to sensitive data and applications?
- What is the process for reporting a potential computer security incident?
- How is the self-reporting by staff of potential computer security incidents encouraged?
- What is the consequence if someone violates security procedures?

Items to observe

- Check the computer access agreement/user policy;
- Verify the training certification/records on computer security;
- Check the account status according to the job for a random selection of employees/contractors (e.g. check the formal authorization for employees involved in a safety system);
- Check the account status of employees that have recently left the organization.
- Are penalties adequate and correctly applied? Is good behaviour appropriately rewarded?
- Do all computers show a 'Notice of Use Agreement' or 'Technology Acceptable Use Policy' during logon?
- Do computers, where appropriate, have a password protected screen saver? What is the time delay?

Field analysis hints

- Could one, or a few, individuals represent the risk of a single point of failure in the process?
- How are access rights for transferred or terminated individuals managed?
- How does the organization promote an active computer security culture in the company? Does it extend to behaviour outside the work environment, e.g. the use of social media?

5.6. PHYSICAL PROTECTION

System domain description

The objective of this domain is to ensure the physical protection of computer assets. It seeks to prevent unauthorized physical access to systems where sabotage could cause disruption or denial of services or information flow. Prevention and security controls are to be based on a risk assessment and implemented according to a graded approach. Due care needs to be taken to mitigate the insider threat.

For I&C systems, implementation of physical controls is often the only way to enforce access control; technical controls may not exist or be relevant for these systems.

Documents and records of interest

- Facility physical security (or protection) policy/plan;
- Computer security policy/plan;
- Functional diagram of systems and associated computer assets;
- Diagram of the physical layout of the facilities;
- Listing/diagram of the physical location of inventoried assets;
- Diagram/listing of physical controls;

— Physical network cables/wiring diagrams;
— Procedures for relevant physical access control processes and access list management;
— Access control logs for physical access to spaces and equipment;
— Organization charts and job descriptions.

Documents and records analysis hints

— Consistency between technical controls, administrative controls, and physical controls;
— Consistency between function sensitivity and the physical protection of the systems/components involved;
— Appropriate computer security of the systems in charge of physical protection;
— Appropriate computer security of the systems responsible for environmental control;
— Verification of appropriate physical separation of different security level networks/components/equipment;
— Has the threat been characterized and are the implemented controls adequate?
— Identify access restrictions that are based exclusively on procedures (i.e. administrative controls).

Sample interview questions

— What are the designated controlled/sensitive areas?
— Describe the technical and procedural access control mechanisms in place for each controlled/sensitive area;
— Are physical protection measures adequate for the computer systems of concern?
— What are the organization's perceived physical threats (including in terms of resources and motives and including insider threat)?
— What is the access or escort policy for third parties working in controlled areas?
— What is the policy for portable media and handheld electronic devices in controlled areas?
— What is the disposal process for broken or replaced computer equipment?
— What is the disposal process for electronic media?
— What is the procedure for removing computer equipment and media off site (e.g. taking a laptop home to do work)?
— What is the procedure for bringing external (i.e. non-facility owned) equipment to use at work, such as a laptop, a thumb drive, etc.?
— What are the physical and administrative controls associated with protecting the computer environment?

Items to observe

— Observe access control enforcement means and procedures in operation.

— Check that personnel authorized for physical access are kept to the minimum. An access control list of those persons having authorized access needs to be maintained and available to security personnel.

— Observe cable and wire protection, cabinets, racks, patch boards and how cables are bound together. Keep in mind that network equipment may be located in multi-purpose areas, not only in server rooms. Is the equipment in a secure area? Who has access?

— What equipment security devices are in place, such as tamper detection devices, physical locking devices, alarms, video surveillance, etc.?

— Observe the application of procedural protection measures (badges, escorts, painted lines not to be crossed, two-person rules enforcement, etc.).

— Observe the use of personal IT devices such as smart phones, laptops, tablet PCs, portable media, etc.).

— Observe the location of computer terminals: are they situated to prevent unauthorized viewing of screens and keyboards?

— Are computer media left on desk unattended?

— What are the security measures in place around supporting infrastructure for the computing infrastructure (i.e. security controls for ventilation and cooling, primary and backup power, etc.)?

— How are individual pieces of equipment tagged, inventoried and tracked?

Field analysis hints

— Analyse physical controls and administrative controls in conjunction;

— Consider the insider threat, and what can be accomplished with physical access to computing resources;

— Observe people bringing in personal computing devices such as smart phones, laptops, tablet PCs, portable media, etc.);

— Check for consistency between logical access control and physical access control.

— Check whether physical access to (selected) I&C systems is connected to an alarm. Where does it alarm to? What are the normal actions for an alarm?

5.7. COMMUNICATIONS AND COMPUTER OPERATIONS MANAGEMENT

Security domain description

The main objective of this security domain is to control the exfiltration and infiltration of data from and to computer systems within the computer security programme to protect against the introduction of new vulnerabilities and to control the operational procedures to ensure that the systems operate and protect as intended. A further objective is to protect the integrity of the computers and communications.

Documents and records of interest

— Data flow diagrams to identify the interconnection between networks and data flow;

— Policy and procedure for configuration management;

— Network architecture diagram;

— Policy and procedure for reconfiguring the computers/networks;

— Policy and procedure for computer system hardening;

— Policy and procedure for media: accessing media, labelling, storage, transportation and sanitation;

— Policy and procedure for verifying and validating security controls implemented on computers and networks within the scope of the computer security programmes;

— Qualification/certification records for the individuals performing the verification and validation testing;

— Policy and procedure for releasing information externally/to the public (e.g. on a corporate website);

— Policy and procedure for handing publicly available information;

— Policy and procedure for third-party service delivery management for all classes of computers and networks within the scope of the computer security programme;

— Agreements with third parties regarding which networks within the facility may be accessed by the third party and third-party security solutions;

— Policy and procedure for dealing with third-party contractors;

— Policy and procedure for continual monitoring and assessment of the computer security programme;

— Policy and procedure for the digital exchange of information within the facilities and with external facilities;

— Policy, procedure for exemptions to the computer security programme, including records of these;

— Policy and procedure for using wireless devices, mobile devices, or removable media;

— Policy and procedure for usage restrictions and implementation for wireless technologies;

— Policy and procedure for conducting scans for unauthorized wireless connections and wireless access points;

— Policy and procedure for handling the discovery of unauthorized wireless connections or access points;

— Policy and procedure for using portable computing devices, including mobile phones;

— Policy and procedure for continuously monitoring and assessing insecure and rogue network connections;

— Policy and procedure and description of methods used to detect unauthorized use of, or access to, systems and/or networks;

— It might also be of value to perform a search on open source information to evaluate publicly available information on the facility or organization that could potentially pose a computer security risk.

Documents and records analysis hints

— Review approved procedures performed by operations and maintenance staff for intrinsic security, and consistency with the security policy and plan.

— Do security procedures address different modes of operation of the facility to capture different security concerns associated with them?

— Do the collected procedures cover the security concerns that they are developed to protect?

— Has the host facility carried out effective analysis to ensure that those security controls operate and protect as they are intended?

— Has the host facility evaluated the impact of a successful defeat of security controls within the communications and operations management domain?

— Has the host facility evaluated the impact of a successful defeat of security controls associated with remote or third-party activities (including maintenance)?

— Has the host facility configured its computers to address currently known vulnerabilities?

— Is the concept of 'least privilege' implemented?

— Does the host facility have a security analysis and testing programme (using vulnerability analysis, penetration testing or other means) to identify potential known and unknown vulnerabilities? What is the scope of the testing programme?

— Are there requirements for contractors and subcontractors to apply the computer security policy?

Sample interview questions

— What is the procedure for removing computer equipment and media off site (e.g. bringing a laptop home to do work)?

— What is the procedure for bringing external (i.e. non-facility-owned) equipment to use on site such as a laptop, a thumb drive, smartphone, etc.?

Items to observe

— Verify that the host facility has configured its computers to support least privilege and a process to analyse and mitigate currently known vulnerabilities;

— Observe the performance of procedures;

— Identify any indication of external entities or connectivity (e.g. for backup or monitoring);

— Spot-check for notebook/mobile devices and inquire about their usage;

— Check for consistency between documented systems, applications, network architecture, etc. and what is actually in place.

Field analysis hints

— Consider whether the risk analysis is comprehensive in identifying the risks associated with network communications and mobile devices.

— Consider the question: what is the biggest remaining challenge?

5.8. COMPUTER ACCESS CONTROLS

Security domain description

The objective is to control logical access (by technical and administrative controls) to computer systems or electronic information.

This domain addresses requirements for access control, user access management, user responsibilities, network access control, operating system access control, application and information access control, and mobile computing and teleworking.

Access to computer systems (I&C systems, supervision systems, technical systems, security systems and business systems) is controlled on the basis of the computer security plan.

Computer and network logical access control rules are specified through a formal authorization process.

Documents and records of interest

— Computer security plan;

— Policy and procedure for computer access control (management of rights, account management);

— Record of results of any access control audits;

— Policy and procedure for reviewing authorization of system access, including privileges;

— Organization chart for computer administrative rights management;

— Policy and procedure for passwords (complexity, duration, and account lockout policy);

— Policy and procedure for privilege granting procedures and documentation;

— Description of employed authentication mechanisms;

— Access control logging and monitoring documentation;

— Policy and procedure for account authorization and accounting;

— Network access policy — switches security, unconnected sockets, etc.;

— Network access policy — usage of virtual LANs;

— Network and traffic topologies;

— Security gateway policy — router access control lists, firewall rules;

— Diagram/listing of wireless access points;

— Policy and procedure for remote access (who, when, why, which services);

— Policy and procedure for modem use and security;

— Policy and procedure for administrative/high privilege accounts.

Documents and records analysis hints

- In instances where required technical access control measures, (e.g. passwords) cannot be implemented within certain I&C components, either for technical or operational performance reasons, verify that corrective measures are employed (e.g. adapted procedures, increased physical security, personnel security, intrusion detection, and auditing measures) according to the security level of the I&C system;
- Check consistency between technical controls, administrative controls and physical controls;
- For I&C systems, pay particular attention to remote access methods and instances where wireless and mobile technologies have been implemented.
- For wireless technologies, is there a usage policy for access and an assessment program to ensure adherence to this policy?
- Check for the application of 'segregation of duties' and 'least privilege' policies, technical or administrative. Specifically, for I&C and essential legacy systems, check that there are corrective measures if not applied.

Sample interview questions

- Which systems are accessed by personnel performing specific job functions?
- Which of these systems are accessed remotely? With what frequency? Why are these systems accessed remotely?
- Check if there is outside-the-procedure delegation or granting of access rights.
- What is the perception of the access control policy: is it too strict, too weak etc.? Does it fit with the operational needs?
- Identify regular issues/problems regarding access control not being handled properly (i.e. workarounds).
- What is the process for granting/obtaining computer access? What are the revocation and renewal processes?
- Identify if access controls are circumvented for operational efficiency (or comfort) in some cases
- What are previous incidents — or even anecdotes — regarding access control?
- Does the administrator have two accounts (admin/user)?
- How does the organization handle changes in personnel situations (e.g. change of department, change of duties, etc.)?

Items to observe

- Ask for demonstrations of access control enforcement means and procedures;
- Check if there is outside-the-procedure delegation or granting of access rights;
- Check logical access control lists to ensure that the number of authorized persons with access is kept to the minimum;
- Check for modems and wireless access points;
- Monitor wireless activity;

— Check for accessible connection ports;
— Identify possible connection points for passive monitoring;
— Look for unlocked systems and workstations;
— Look for systems without a password, with default accounts or with an obvious password;
— Check for banners informing users of the authorized types of usage;
— Check how network segregation is achieved (logically, physically, air gapped);
— Check network architecture and especially interfaces between security domains;
— Identify possible paths to compromise critical systems (safety, control) from business or corporate networks, or in other ways;
— Identify regular issues/problems regarding access control not being handled properly (workarounds);
— Look for undocumented authentication mechanisms.
— Look for login procedures; is there a clear text authentication mechanism in place?
— Are accounts and passwords shared among personnel; are there group accounts in use?
— Ask for the schedule of activities during the time of the assessment, and select certain activities to observe, such as patching, parameterization, software installation, etc.

Field analysis hints

— How many different passwords does a person need to use in everyday operations? During special operations? (Too many passwords may lead to use of sticky notes etc.)
— Do personnel log off/lock the account when leaving their computer, if applicable?
— How is traceability handled if group/shared accounts are used?
— How is password complexity ensured?
— What is the consistency between logical access control and physical access control?

5.9. COMPUTER SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE

Security domain description

The objective of this security domain is to ensure the security and integrity of the computer systems being acquired, and maintenance activities performed by the vendor after placing of the system in service. The security controls covered by this security domain include supply chain protection, correctness of software, integration of security capability, factory testing, and acceptance testing.

Special note needs to be taken of maintenance activities on computing systems. Such activities need to be evaluated to ensure they have sufficient controls in place to guard against the introduction of vulnerabilities or malware. Additionally, computer security maintenance activities, such as patch management, are advised to be evaluated for their timeliness and effectiveness.

Documents and records of interest

- Policy and procedure for system and service acquisition including the development of security requirements for the acquired or developed systems;
- Description of requirements to provide security measures to protect against vulnerability and threat introduction via the supply chain;
- Description of requirements for vendors to employ software quality and validation methods to minimize flawed or malformed software;
- Description or demonstration of how the facility ensures that newly acquired systems contain sufficient security design information, capabilities or both to implement and maintain the required security controls;
- Description or demonstration of security requirements to create, implement and document security tests and evaluation plans to ensure that the acquired products meet all specified security requirements;
- Description and demonstration of the security requirement to maintain the integrity of the acquired system until the product is delivered to the facility. Description of how the facility verifies and checks that the security programme implemented before delivery is secure to at least the same level as to that applied to the computer system when in operation.
- Test plan and results for verification and validation of code against the security design and configuration requirements;
- Computer/electronic equipment acceptance test procedures;
- Requirements document for implementation and maintenance of computer security measures;
- Validation test plan and results for evaluating the effectiveness of implemented computer security measures;
- Computer security design and methodology describing security design features developed to address the security requirements identified for the computers;
- Maintenance records for computing systems;
- Maintenance schedules reflecting prioritized computer security related tasks.

Documents and records analysis hints

- Check that computer security is being appropriately addressed by third parties;
- Check for security along the acquisition and development chain, taking into consideration that there may be many contractors, subcontractors, etc.

Sample interview questions

- What controls are placed on equipment on site prior to and during installation?
- What testing occurs to evaluate security functions — at the vendor and after installation?
- What controls are in place to ensure that computer vulnerabilities or exploits such as malware are not inserted into the system during maintenance activities?

— How are third-party maintenance activities monitored on site?

— Evidence of Vendor Site Security Inspections and record of compliance with security requirements.

Items to observe

— What controls are placed on equipment on site prior to and during installation?

— How is sensitive information communicated between the vendor and the facility?

Note: This domain is difficult to observe on site as it mainly relates to third parties before systems are delivered.

Field analysis hints

— Observe a computer security maintenance activity conducted by internal staff or third-party contractors.

5.10. COMPUTER SECURITY INCIDENT MANAGEMENT

Security domain description

A computer security incident may occur despite the best efforts of an organization. The objective of this security domain is to ensure processes are in place for effective mitigation of the potential impact and effective communication of computer security incidents.

According to IAEA Nuclear Security Series No. 17 [3], a computer security incident is an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a computer-based, networked or digital information system, or the information that the system processes, stores, or transmits, or that constitutes a violation or imminent risk of violation of security policies, security procedures, or acceptable use policies.

Documents and records of interest

— Policy and procedure for incident management;

— Incident communication plan;

— IT Helpdesk Requests (Tickets);

— Unplanned Facility or System Shutdown events (Root Cause Evaluations) demonstration of security evaluation;

— Sample or template of an incident report (an actual report would be preferred);

— Procedure/considerations for cross domain effects of an incident response (for instance, actions taken on a business IT system after a security incident may not be acceptable within an I&C environment);

— Incident Response Plan and Procedures;

— Records and subsequent actions resulting from the performance of exercises to evaluate the effectiveness of the incident response plan.

Documents and records analysis hints

— Does the computer security incident management adequately consider external and internal (i.e. insider) threats?

— Is there a clear classification scheme to characterize the incident?

— Is the escalation procedure clearly defined (criteria, point of contacts)?

— The communication process addresses internal communications (including to the overall facility incident management) and external communications (links to Computer Emergency Response Teams (CERTs), national and international authorities).

— Have the procedures for forensics, trace preservation, etc. been developed and adapted to support the investigation process?

— Evaluate the remediation process, and the definition and application of corrective measures;

— Check the consistency between incident management and continuity management;

— Check the link between computer security incident management and overall facility incident management.

— Has the facility performed the incident response plans and procedures as part of a self-assessment exercise (i.e. tabletop or mock exercise)?

— Has the facility participated in any coordinated computer security incident exercises involving external organizations?

— Have evidence preservation and chain of custody requirements been incorporated into the Computer Security Incident Response plan and procedures?

Sample interview questions

— Check knowledge of the procedure, and in particular the point of contact, for employees and contractors when a security incident occurs.

— Describe what constitutes a security incident. How is a security incident categorized?

— When, and under what circumstances, would an incident be reported? To whom, externally, is the incident reported?

— What is the procedure if a deviation in the implementation of security controls is identified by an employee or a contractor?

— Has the facility had any (computer) security incidents?

— Can you describe what has been done or changed following a recent computer security incident?

— Are the existing processes deemed effective? What, if any, challenges still exist?

— How and how often do they exercise the incident response plans and procedures?

— Has the facility participated in any coordinated computer incident exercises at a facility, State or international level?

Items to observe

— Request a demonstration of the specific incident management tracking incident system (paper or software application).

Field analysis hints

— Evaluate whether the staff have received sufficient training on the procedure.

5.11. CONTINUITY MANAGEMENT

Security domain description

The general objective of this security domain is continuity and restoration of a facility's critical functions following major disruptions to normal computer systems and processes. This includes disruptions caused by natural hazards, human error, and malicious intent.

Note that the section on Computer Security Incident Management dealt with the initial response and mitigation of the incident, while this domain's focus is continuity and the recovery process.

Documents and records of interest

— Policy and procedures for continuity management;

— The list of applications and systems that have continuity management, and the list of their owners/responsibilities;

— Continuity of operations training records (including exercise reports);

— Continuity of operations plan.

Documents and records analysis hints

— See how continuity management related to computer security is integrated into the facility's existing operation continuity programmes (for example, via a site business continuity plan);

— Note that continuity management is taken into account in the basic design and technical specifications for I&C safety and operation systems. It is recommended that these specifications are taken into consideration when evaluating continuity management for I&C safety and operation systems. This may not be the case for other functional domains. For I&C systems performing important safety or security functions, Mean Time Between Failure and Mean Time To Repair are two key design attributes that need to be considered in determining continuity management actions;

— Are important subsystems and interdependencies identified? Are contract agreements sufficient to support continuity objectives?

— Important systems and functions have an appropriate level of diversification and redundancy.

— Is the malicious dimension (intentional attack vs. incidental failure) appropriately addressed in the continuity management?

— Check for consistency between incident management and continuity management.

Sample interview questions

- Check if test plans for continuity and recovery of computer systems and recovery procedures (e.g. restore and update of data between a shutdown and restart) are known, tested and reviewed.
- Have staff undergone training on system recovery and continuity management? Who has been trained? How does continuity management address prioritization of access and resources during operational degradation?
- Has the facility conducted training exercises focused on system recovery and continuity management for a cyber-event?
- Do backup systems exist to manage important computer functions if there is an incident/accident?
- What security controls are applied to the backup systems?
- What is the architectural tie to the backup systems?
- Do procedures exist for operation following the loss of computer functions?

Items to observe

- Check that employees have access to the relevant continuity procedures;
- The assessment could select a subset of continuity management controls to review, such as backup and restore procedures, alternative communication means (in particular for the emergency response) and contractors' prioritization agreements;
- Ask for the latest exercise report;
- Observe the alternative and backup control facilities if they exist.

Field analysis hints

- Observe the performance of a recovery procedure, either on the system, in a development lab, or using a "paper" process.
- Is plant configuration information up to date? By which mechanism/process?
- Assess the relevance of the prioritization of access and resources during operational degradation with respect to the overall facility objectives.

5.12. COMPLIANCE

Security domain description

If the assessment is performed by the competent authority, or it is a self-assessment, compliance with relevant legal, statutory, regulatory or contractual obligations related to computer security may be part of the assessment scope.

The objective of this security domain is to check that the computer security programme is in line with these relevant legal, statutory, regulatory or contractual obligations.

Note that this domain may not be applicable in some contexts; this can be considered when planning the assessment scope.

Documents and records of interest

— Legal, statutory, regulatory or contractual obligation documents which address aspects of computer security;

— Regulatory compliance report(s) (internal or external);

— Certification procedures/process if relevant for computer security;

— The computer security component of the Design Basis Threat;

— System design and modification guidance documents (the sections that refer to compliance constraints).

Documents and records analysis hints

— Each functional domain may have different compliance criteria and constraints;

— Moreover, depending on the countries and the type of facilities, there may be several regulatory frameworks to consider, from different state level agencies (for instance, from both the safety regulator and a security agency);

— Aspects of computer security may be embedded in broader scope documents; for instance, there may be dedicated computer security sections within applicable safety standards.

— How are legal and regulatory requirements included in the security policy, organization and procedures?

— Are the related documents clearly referenced or listed in the security policy?

— I&C systems usually have dedicated design and modification guidance documents, but the assessment team may analyse those aspects for the other domains (e.g. nuclear material accountancy, emergency response related systems).

Sample interview questions

— How are regulatory requirements identified, tracked, and implemented?

— Who is responsible for such tasks (identification, tracking and implementation)?

— Explain how field modifications are validated for their impact on compliance with legal, statutory, regulatory and contractual obligations.

Items to observe

— The assessment could select a subset of computer security requirements from legal, statutory, regulatory and contractual obligations and validate field implementation.

Field analysis hints

— Start with a small representative sample; if several discrepancies are identified, the sample can be revisited and additional elements examined.

6. FINAL REPORT AND POST-ASSESSMENT ACTIVITIES

6.1. DEVELOPING THE FINAL REPORT

One of the most important aspects of the assessment is the discussion of the observations, determination of findings, recommendations and suggestions provided to the host organization. This information is captured in the final report and presented in an exit briefing to the host facility or organization.

The report format and content may vary depending upon the purpose of the assessment, but contain consistent elements such as an Executive Summary, Introduction, Results and Conclusion sections. Annex III provides an example of an assessment report. Figure 3 illustrates the process that goes into the report preparation and development.

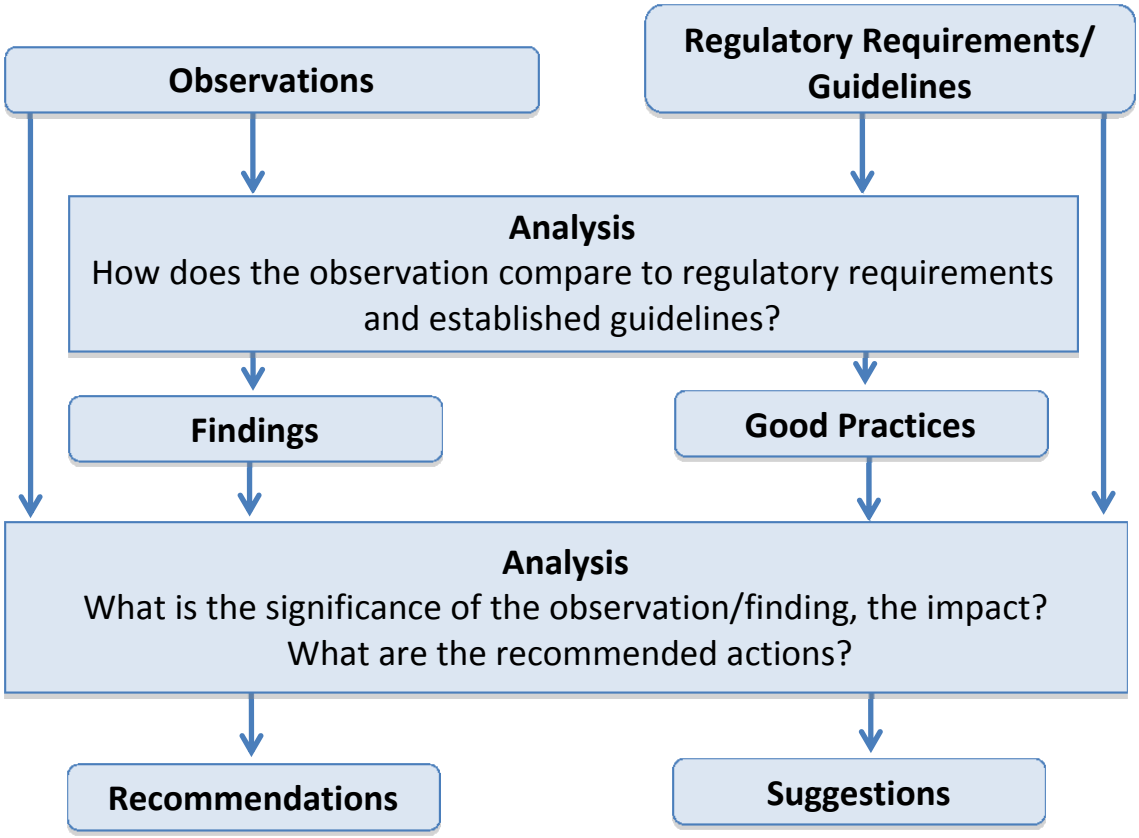

FIG 3. The assessment analysis process.

The data collection component of the assessment consists of recording the observations of data of interest found during the document/record review, interviews and direct observations. Observations are individually significant, but may also act as a collective indicator of trends at the facility or organization that may need to be addressed. During the review of field notes, similar observations may be grouped together to indicate trends or recurring instances.

The observations are then analysed against requirements such as national regulations, organizational procedures and/or international standards as appropriate. A finding is determined if there is noncompliance with, or variance from, a regulatory or internal procedure. The basis used for finding determination needs to be well defined and agreed in the preliminary planning meetings.

It is also important to understand that the list of findings is only a snapshot view of the facility based on a number of observations conducted by the assessment team. The analysis of observations and the development of findings must take into account multiple factors including:

— The depth and breadth of the assessment;

— The skill and experience of the assessment team;

— The level of access given to the assessment team;

— The level of resources given to the assessment, e.g. time and number of assessors.

The assessment findings will therefore represent a selective sampling and not an exhaustive representation of the computer security practices of the organization. A finding confirms the presence of an issue, but the lack of findings does not mean computer security issues do not exist.

Observations do not always result in findings and not all findings are adverse. One additional outcome is the identification of 'good practice', i.e. an organizational process or procedure that provides a novel and effective method for meeting security objectives. Such practices are to be identified and reported as potential examples for other organizations to improve their own security programmes.

In addition to findings and good practice, the assessment team may also provide additional guidance, recommendations and suggestions in the report associated with the findings.

Recommendations provide conformance guidelines for legal and regulatory requirements (national laws/regulations) and/or international norms, when appropriate. Recommendations do not normally provide information on how to correct a problem, and indicate only that a problem needs to be corrected.

Suggestions provide an additional level of information regarding a finding, including corrective or mitigation strategies. Such information is not necessarily derived from regulatory guidance, but rather from technical standards and industry good practice.

Suggestions may include actions such as:

— Modifications to equipment and the installation of additional devices and means to improve security;

— Improvement of procedures and administrative measures;

— Development of additional checks and controls;

— Rectifying deficiencies revealed in the operational procedures;

— Rectifying deficiencies in policy documents;

— Training personnel in both general and specific job functions;

— Making changes to the working environment;

— Making changes to the planning and scheduling of work and/or to the individuals assigned to particular duties.

6.1.1. Significance analysis

In an assessment, it is often not enough to identify a finding; ultimately, the impact or potential consequence of the finding must be explored. The host organization needs to consider the impact or significance of the finding for security and safety. Impact analysis may

be conducted at multiple levels. The first level examines the impact of the individual finding, specifically looking at its impact or significance with regards to CIA attributes (confidentiality, integrity and availability). The second level of analysis takes a systematic view and examines the set of findings and the overall effect that they have on a facility or organization. Such an analysis is non-trivial and will require a multidisciplinary team to look at all of the ramifications for safety, security, operations, etc.

This level of analysis is not typically conducted by the assessment team for a regulatory review in which the analysis is left to the host organization. However, such analysis may be conducted jointly with the assessment team for self-assessments or third-party technical advisory missions. Such assessments take significant resources and time to conduct.

6.2. REPORTING ELEMENTS

Depending on the arrangements for the assessment, reporting may be carried out during the assessment, e.g. a draft report is made available for the exit briefing, or provided afterwards.

The following considerations are to be taken into account regarding the content of the report:

- Team members need to be objective, basing their conclusions on their review of pertinent documents, the interview of key personnel, and direct observation;
- Team members need to consult their host counterparts to clarify any area that is in question and ensure that it is correctly understood;
- Team members need to consult with each other, and particularly the Team Leader, and share the results of their findings in order to avoid duplication, inconsistency and areas that may impinge on other findings;
- Team members' conclusions — in particular those resulting in recommendations, suggestions and the recognition of good practice — need to be concisely documented and supported by a 'basis' which forms the foundation for justifying a particular recommendation, suggestion, or good practice;
- The sensitivity of the final report needs to be considered, based on the sensitivity of its content, the vulnerabilities it may expose (and the potential consequences of these), and any applicable national or organizational policy on sensitive information. The sensitivity of the report needs to be clearly marked on the document, and the report needs to be handled accordingly.

When reporting a finding, the report needs to be clear and if possible state the following:

- The relevant function and security domains (multiple domains may be impacted);
- The guidance and/or good practice used for evaluation (citing the reference for the guidance);
- The finding;
- The potential impact of the finding (this could be viewed as a severity rating, e.g. administrative, minor, major, severe, etc.);
- The recommended solution or remedial action.

Findings may be further aggregated across functions and security domains for a general grading or evaluation of the collective areas.

The report indicates the team's level of confidence that the assessment was sufficiently comprehensive to provide a true evaluation of the facility.

Areas that were not evaluated are to be identified.

Regarding formatting and the style of the report, the following considerations may be of help:

— An initial summary outlining the general impressions that the team gained from the review can be useful in providing a perspective for the subsequent, more detailed, discussion of the individual areas.

— Language needs to be simple, clear, concise, objective and impersonal.

— Charts and photographs may be inserted in the section they apply to. Figures illustrating a government or organization — and diagrams or photographs that illustrate a deficiency or a good practice — are particularly useful.

— Official names (or official translations) are used to designate organizational units, positions and systems.

— Abbreviations are to be introduced when first used, and listed and defined in a separate table for easy reference.

6.3. EXIT BRIEFING

Participants in the exit briefing include people from the assessed entity, and may also include other parties. If necessary, the assessment team leader will advise the assessed entity of any situations encountered during the assessment that may decrease the reliance that can be placed on the assessment conclusions. The assessment meeting is formal, so minutes and records of attendance are to be kept.

REFERENCES

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

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities, IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

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

[4] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary, ISO/IEC 27000:2009, ISO, Geneva (2009).

[5] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Information Security Management Systems — Requirements, ISO/IEC 27001:2005, ISO, Geneva (2005).

[6] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Code of Practice for Information Security Management, ISO/IEC 27002:2005, ISO, Geneva (2005).

[7] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Information Security Risk Management, ISO/IEC 27005:2008, ISO, Geneva (2008).

[8] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Requirements for Bodies Providing Audit and Certification of Information Security Management Systems, ISO/IEC 27006:2007, ISO, Geneva (2007).

[9] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Guidelines for auditing management systems, ISO 19011:2011, ISO, Geneva (2011).

[10] UNITED STATES NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Technical Guide to Information Security Testing and Assessment, NIST Special Publication 800–115, Gaithersburg, Maryland, USA (2008).

GLOSSARY

Terms used in this publication are defined below. When available, definitions are taken from existing IAEA publications or international standards. Where this is the case, the definition includes a reference to the originating publication (listed in the Reference section at the end of the main document).

Assessment. The methodology described in this publication is an activity which, for simplicity and consistency, is referred to throughout as an 'assessment'. But, as noted above, this methodology may be applied in various contexts, and other descriptions of the activity may be appropriate, such as 'advisory service', 'expert visit', 'audit' or 'self-assessment'. Use of the term 'assessment' is not to be construed as allocating any additional authority or responsibility to the IAEA or any other organization conducting an assessment.

Computers and computer systems. The computation, communication, and instrumentation and control devices that make up functional elements of the nuclear facility. These include not only desktop computers, main frame systems, servers and network devices, but also lower level components such as embedded systems and PLCs (programmable logic controllers). In industrial settings, such computer systems may be referred to as industrial control systems (ICS) and, in nuclear power plants, as nuclear instrumentation and control (I&C) systems.

Computer security. A particular aspect of information security that is concerned with computer based systems, networks, and digital systems [3]

In this publication, the term 'computer security' refers to the security of all computers as defined above and all interconnected systems and networks. (The terms 'IT security' and 'cyber security' are considered to be synonyms but will not be used here)

Finding. An observation where there is variance between how something is carried out and how it is supposed to be carried out according to regulatory requirement, standard or good practice.

Good practice. Good practice is a programme, activity, way of using equipment, etc. that has proven to be outstanding and contributes directly or indirectly to operational safety or security, as well as sustained good performance. Good practice is markedly superior to expected behaviour, and is not just the fulfilment of current requirements.

Observation. Something identified as the result of a document review, an interview or a direct observation.

Recommendation. An action that reinforces the security of a nuclear facility (for a host assessment); a mandatory enforcement action to address a finding (e.g. from a State's regulatory body).

A recommendation is advice that is strongly encouraged to be followed for the activity or programme being assessed in order to improve operational security. It is based on IAEA Nuclear Security Series guidance, national regulations, standards or international proven good practice, and it addresses the root causes of an issue rather than just the symptoms. A recommendation often encapsulates a proven method of striving for excellence, reaching beyond minimum requirements. It needs to be specific, realistic and designed to result in a tangible improvement.

The use of the term ‘recommendation’ in this publication is not to be confused with its meaning in regard to guidance found within the Nuclear Security Series publications.

Requirement. The basis for a specific assessment, i.e. the rules, regulations and standards to be followed.

Suggestion. A proposed action or enhancement that the assessed nuclear facility could implement.

A suggestion may be an addition to a recommendation or may stand on its own. It may indirectly contribute to improvements in operational security but a suggestion is primarily intended to make good performance more effective, to indicate a useful expansion to an existing programme or to point out a possible superior alternative to ongoing work. In general, a suggestion is designed to stimulate the plant’s management and staff to continue to consider ways to enhance performance.

ANNEX I
HINTS FOR INSTRUMENTATION AND CONTROL SYSTEM ASSESSMENT

INSTRUMENTATION AND CONTROL SYSTEM OVERVIEW

In the context of this publication, the terms ‘computers’ and ‘computer systems’ refer to the computation, communication, and instrumentation and control devices that make up functional elements of the nuclear facility. They include not only desktop computers, mainframe systems, servers and network devices, but also lower level components such as embedded systems and PLCs (programmable logic controllers). A subset of these computing systems includes digital control and instrumentation and control systems. These are particularly important for evaluation during the assessment as their compromise can have severe effect on both security and safety.

The instrumentation and control (I&C) system serves as the operational backbone for facility processes. IAEA Nuclear Energy Series NP–T–3.12 (Ref. [I-1], pp 2–3) details three basic functions provided by the I&C system over plant processes. The first is to provide the sensory capabilities (e.g. measurement and surveillance) to support functions such as monitoring or control and to enable plant personnel to assess its status. Thus, I&C systems such as sensors and detectors are the direct interfaces with the physical processes in the nuclear power plant and their signals are sent through communication systems to the operator, as well as to the decision-making applications (analogue or computer based).

The second function is to provide automatic control, both of the main plant and of many ancillary systems. The third function of the I&C system is to respond to failures and off-normal events, providing safety and protecting the plant from the consequences of any malfunction or deficiency of plant systems or as a result of manual errors.

These computing and associated (I&C) systems used in the operational functions of a nuclear power plant, a fuel cycle, or storage facility, support a variety of functions and exist under multiple names in industry. Here the term ‘industrial control systems’ (ICS) is used to describe these systems, which include: supervisory control and data acquisition (SCADA) systems, distributed control systems, and other control system configurations such as skid-mounted Programmable Logic Controllers [I-2].

Control components within the ICS may include (Ref. [I-2], pp 2–4):

— Remote Terminal Units to support remote device control and monitoring;

— Programmable Logic Controllers, which are small computers often used to control industrial processes;

— Intelligent Electronic Devices, which are smart sensors/actuators for local data acquisition, communication, and local control;

— Human–Machine Interface/Human–System Interface, which provide the interface for a human to monitor and control plant processes.

These systems exist as part of the ICS network, which also contains standard and specialized network components such as routers, firewalls, servers, modems and remote access points.

The control network then interfaces with the lower level components such as sensors and actuating devices to control and/or monitor plant processes, as shown in Fig. I-1.

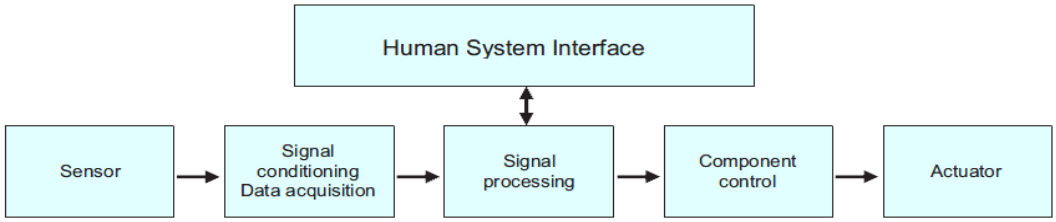

FIG. I-1. Block diagram of a typical I&C function [I-1].

Multiple identical processes may be controlled on one network. Conversely, processes may be managed on entirely separate networks. In the control network, each of these individual components is a potential vulnerable point of the system and therefore needs to be addressed at some level within the assessment. One challenge is that these components were not necessarily designed with computer security as a consideration.

CONTROL SYSTEM COMMON VULNERABILITIES

The following lists common vulnerabilities identified by the US Department of Homeland Security [I-3], which may be considered in developing and conducting the assessment of a facility's ICS and I&C systems. No single item may, in and of itself, necessarily be grounds for concern, but rather individual items need to be considered in the overall context of the assessment. Compensating controls or nested defensive mechanisms may have already addressed these potential issues.

Access control

- Access is not restricted to the objects that require it;
- ICS protocol allowed ICS system hosts to read or overwrite files on other hosts, without any logging;
- Documentation and configuration information was being shared freely (read only);
- Common shares are available on multiple systems;
- A lack of role-based authentication for ICS component communication;
- A remote user can upload a file to any location on the targeted computer;
- Arbitrary file download is allowed on ICS hosts;
- Arbitrary file upload is allowed on ICS hosts;
- A remote client is allowed to launch any process;
- And ICS service allows anonymous access;
- Undisclosed 'back door' administrative accounts for future vendor access to perform maintenance, updates, or training;
- Manager account overused;
- Remote exploitation of ICS application services allowed root level access on ICS hosts;
- Database service running as administrator;
- Authentication is not required to read a system configuration file that contains user accounts details, including passwords;

— Lack of separation of duties through assigned access authorization;
— Lack of lockout system enforcement for failed login attempts.

Passwords

— Some ICS hosts had very weak three character administrative passwords;
— The weak passwords were recovered and provided root-level access to all system resources;
— Several weak passwords were found;
— The default password had not been changed;
— Default administrator level user names and passwords are in use;
— Default credentials are assigned to several predefined user accounts on the device, including the administrative user account;
— And ICS component is directly accessible from the Internet using the default username and password;
— The length, strength and complexity of passwords is not enforced;
— Many of the accounts, including the administrator account, had no password expiration date;
— Account lockout policy not defined;
— Password complexity has been disabled;
— Password history set to remember zero previous passwords.

Code artefacts

The storage of ICS, such as source code and system configuration on a shared file system, provides significant potential for information mining by an attacker. The design of many ICSs includes open network shares on ICS hosts. The following are examples of assessment findings associated with this vulnerability:

— Publically available network shares on ICS Hosts. Two shares were discovered on work station and server computers;
— Common shares on multiple systems;
— Files available for read access;
— Information leak through shared directories;
— A large number of publically available network shares on ICS hosts;
— The source code for the ICS is shared on ICS hosts. The source code could be downloaded and used to find vulnerabilities.

Patch management

Unpatched or old versions of third-party applications incorporated into ICS software were found with the following:

— Vulnerable database version;

— Vulnerable web server version;

— Object Linking and Embedding for Process Control OPC relies on Remote Procedure Call (RPC) and Distributed Component Object Model (DCOM); without updated patches, OPC is vulnerable to the known RPC/DCOM vulnerabilities;

— Vulnerable (unpatched) SSL libraries.

Planning/policy/procedures

— Lack of formal documentation;

— Poor security documentation maintenance;

— Lack of an established computer security team;

— Lack of disaster recovery policies;

— Lack of understanding of recovery procedures;

— Weak backup and restore abilities;

Network design weakness

General

— No security perimeter defined;

— Network devices not properly configured;

— Port security not implemented on network devices.

Lack of network segmentation

— Control networks used for non-control traffic;

— Control network services not within the control network;

— Lack of internal segmentation of the ICS production network: Inter-Control Center Communications Protocol (ICCP) servers not on DMZ;

— Lack of internal segmentation of the ICS production network: host with dedicated serial link for data transfer using high risk application not on DMZ;

— Control related systems are accessible on the corporate LAN;

— Incident response and on-site CSET assessments identified the following problems at multiple sites;

— Control networks used for non-control traffic;

— Control network services not within the control network.

Firewalls/DMZ

— Firewalls non-existent;

— Lack of functional DMZ;

— Physical cables connected directly to the ICS LAN, bypassing the firewall;

— SSH server bridges corporate and ICS LANs, bypassing the firewall;

— Third network card on ICCP server connects directly to ICS LAN;

— Access to specific ports on host not restricted to Required IP addresses;
— Access lists are defined but not applied. No inbound filtering;
— Access lists are incorrect for the required ports;
— Access to network printer services on corporate LAN was not restricted by password protection or access control list;
— Email client on DMZ had access to corporate LAN and Internet;
— Inadequate outgoing access restrictions;
— Firewall rules are not tailored to ICS traffic.

Audits and accountability

— Lack of security audits/assessments;
— Lack of logging or poor logging;
— Network architecture not well understood;
— Weak enforcement of remote login policies;
— Weak control of incoming and outgoing media;
— Insufficient method for monitoring control network events.

ANNEX I REFERENCES

[I-1] INTERNATIONAL ATOMIC ENERGY AGENCY, Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants, IAEA Nuclear Energy Series No. NP–T–3.12, IAEA, Vienna (2011).

[I-2] UNITED STATES NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800–82, Gaithersburg, Maryland, USA (2011).

[I-3] UNITED STATES DEPARTMENT OF HOMELAND SECURITY, Common Cybersecurity Vulnerabilities in Industrial Control Systems, US Department of Homeland Security, (2011), available online at:

https://ics-cert.us-cert.gov/sites/default/files/documents/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf

ANNEX II

TEMPLATE FOR OBSERVATIONS

The following example templates are provided as aides to assist assessors in the collection and analysis of the data for an assessment.

These templates and the data tables are only intended to be examples and may be modified to fit the needs of the assessment team.

The observations will be used to build the final assessment report.

Assessor name			**Number**		
Date and time					
Location	Where the observation takes place				
Facility	If applicable				
System	If applicable				
Security domain	As per definition				
Functional domain	As per definition				
Security level					
Observation:	Describe what was observed or identified				
How identified	Document Review	Interview	Observation	Open source	Other:
Intent	Recommendation	Suggestion	Good practice	Other :	
Finding*	Describe the variance				
Basis*	Reference to IAEA guidance, good practice, standard, regulation, known attack vector, etc.				
Root cause*	Reason the problem exists				
Exploitability*	easy	moderate	complex		
Accessibility*	Outsider threat/insider threat (knowing or unknowing)				
Potential impact*	Description of the direct and indirect impact of the finding.				
Significance level*	Categorization of the finding based upon its potential impact (Organizations may devise their own significance or impact scale)				
Action*	Implement good practice, implement standard, implement regulation, patch system, etc.				
NOTES:					

* These items may not be immediately evident during the observations and may be completed later.

Field Template Legend

Functional domains

OP: Operations Domain

BU: Business Domain

SA: Safety Domain

PP: Physical Protection Domain

ER: Emergency Response Domain

Security domains

SP: Security Policy

OI: Organizing Information Security

AM: Asset Management

HR: Human Resources Security

PP: Physical Protection

CO: Communications and Operations Management

CA: Computer Access Control

CM: Computer Systems Acquisition, Development and Maintenance

CI: Computer Security Incident Management

CM: Continuity Management Compliance Emergency Response

CP: Compliance

Exploitability

Easy	Vulnerability generally known; public exploits exist
Moderate	Some details known; proof of concept available
Complex	No details available

Potential types of actions

Modifications to equipment and the installation of additional devices and means to prevent the recurrence of the same or similar events.

Improvements of procedures and administrative measures, and additional checks and controls.

Rectifying deficiencies revealed in the operation documentation (operation manuals).

Rectifying deficiencies in normative documents.

Training personnel to perform jobs properly.

Making changes to the working environment.

Making changes to the planning and scheduling of work and/or to the individuals assigned to particular duties.

ANNEX III

FINAL REPORT TEMPLATE

EXECUTIVE SUMMARY

The executive summary briefly and concisely describes the context, objectives, methodology and requirements, major recommendations and good practice.

INTRODUCTION

- Objectives;
- Scope;
- Simplified network architecture map to ensure that the assessment team and host organization have a shared understanding of the assessment boundaries;
- Methodology;
- Definitions (if needed).

ASSESSMENT RESULTS

Findings

- Findings are obtained by applying requirements filters on the observations. Findings are to be listed;
- Requirements documents such as regulations, procedures, standards, good practice etc. are to be defined and their identification needs to be mentioned with the finding;
- Observations may or may not be included, but may be referenced for the findings (or may be excluded if already communicated to the facility).

Recommendations, suggestions and good practice

- Recommendations (for findings) and suggestions are to be defined and mapped to the referenced requirements or guideline;
- If the assessment is performed by a State or a Regulatory Agency, recommendations may be defined precisely as, for example, Directives, Action Notices, etc.;
- Recommendations may be ranked according to a graded approach related to the potential risk or impact to the facility. The basis for ranking is to be discussed and agreed in the pre-assessment meeting.

Mitigation strategy (optional)

- Adding a mitigation strategy section is an option that can be discussed prior to the assessment;
- If a mitigation strategy is to be included in the final report, the contents of this section is to be discussed with the facility staff.

Impact analysis (optional)

— An analysis related to the potential impact of findings on the facility's functional areas such as Safety, Physical Security, Radiation Protection, etc. may be included in the report. This analysis will not be a component of all assessments and the level of the analysis needs to be discussed and agreed in the planning meeting.

CONCLUSION

This section gives an overview of the assessment result and restates the major recommendations, suggestions and good practice towards requirements and nuclear facility risk analysis. If a mitigation strategy is included in the final report, a major action plan can be added.

REFERENCES

List of relevant documents/references used for the assessment and analysis:

— Requirements;
— Regulatory guides;
— Standards;
— Procedures, any other document used, etc.;
— Employee interviews;
— Functional positions interviewed (manager, engineer, technician, etc.).

ABBREVIATIONS

ANNEX

— Assessment schedule;
— Observation forms;
— Findings forms.

ANNEX IV

CONSIDERATIONS FOR ADDRESSING REPORT RESULTS

This Annex provides aspects for the host organization to consider when addressing the results found in the assessment's final report. The report will contain a combination of findings, observations, recommendations, and suggestions. Each organization will have its own processes for developing an action plan based on these results.

Multiple levels of management including senior management need to be involved in reviewing the report. This is important to ensure that proper emphasis and resources are dedicated to developing an action plan. Some correction or mitigation actions may be straightforward, but others may require detailed analysis. The following considerations may be helpful in supporting the decision-making process for developing this action plan.

Impact

- What is the prime impact of the report for the organization?
- How does the report affect the overall organizational risk profile?

Mitigation

- What additional information is needed to make a decision?
- What is the effectiveness of the proposed solution? (What is the risk reduction?)
- Can multiple findings be addressed with one solution?
- What is the impact of implementing the recommended solution (e.g. does implementing the solution have adverse side effects such as invalidating system certification, licensing or warrantees)?
- Does the proposed solution impose additional or different risks?
- What alternative measures are there to the recommended solution?
- How can the organization verify the proposed recommendation is effective?

Mitigation timeframe

- What is the timeframe for implementing the recommendation? Is this sufficient to address the threat?
- What special conditions are required to implement the solution (e.g. a shutdown or a maintenance period)?
- Can the finding be addressed using interim measures until more permanent measures are in place?
- Are there organizational plans for future projects that address or modify the issues, or that provides an opportunity for addressing the issue?

Mitigation costs

- Does the organization have the technical skill and expertise to implement the recommendation?

- What do the proposed solution costs include?
  - Acquisition costs;
  - Implementation costs;
  - Communication costs for the new solution;
  - Training costs for staff;
  - Training costs for users;
  - Costs to productivity and convenience;
  - Costs for auditing and verifying effectiveness;
  - Disposal costs at the end of life.

Communications

- Is it of value to notify external organizations, e.g. vendors, industry partners or competent authorities, of specific report results?
- If the assessment is part of the regulatory process, reporting requirements for the action plan and follow-on actions may be required by the competent authority.

Other considerations

- Is this a reoccurring finding, perhaps implying the issue was not adequately addressed or the previous measure was not effective?
- Is the collection of findings symptomatic of a larger organizational issue?
- How can the organization prevent reoccurrence of this or related findings in the future?
- How will report results and the action plan be tracked within the organization?

IAEA
International Atomic Energy Agency

No. 24

ORDERING LOCALLY

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

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

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

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

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

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

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

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

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

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

HUNGARY
Librotrade Ltd., Book Import
Pesti ut 237. 1173 Budapest, HUNGARY
Telephone: +36 1 254-0-269 • Fax: +36 1 254-0-274
Email: books@librotrade.hu • Web site: http://www.librotrade.hu

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

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

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

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

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

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

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

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

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

International Atomic Energy Agency
Vienna
ISBN 978–92–0–104616–1