



**The Inspection Technology and
Quality Assurance National Institute**

**HAZARD ANALYSIS RISK AND
OPPORTUNITY ASSESSMENT
PROCEDURE
ITQAN-MP-02**

According to the ISO 9001:2015 ISO 14001:2015 and ISO 45001:2018

ITQAN Institute



HAZARD ANALYSIS RISK AND OPPORTUNITY ASSESSMENT PROCEDURE

| | |
|-------------|--|
| Document ID | Hazard Analysis Risk and Opportunity Assessment Procedure ITQAN-MP-02 |
| Date | Aug 2023 |
| Prepared by | Training Operation Officer |
| Reviewed by | ITQAN Management |
| Approved by | ITQAN Managing Director |
| Version | 1.0 |
| Responsible | |

COPYRIGHT

This procedure is the property of Inspection Technology and Quality Assurance National Institute. No part of this procedure may be reproduced in any form by print, photocopy, microfilm, or any other means wholly or in part or disclosed to any person outside Inspection Technology and Quality Assurance National Institute without the written permission of the Director. Any query about this document should be addressed to the Management Representative of Inspection Technology and Quality Assurance National Institute.

HAZARD ANALYSIS RISK AND OPPORTUNITY ASSESSMENT PROCEDURE

1. PURPOSE

The main purpose of this procedure is to establish a systematic approach to identify and analyse hazards, incidents, risks, and opportunities within ITQAN's operations. The goal is to reduce risks to acceptable levels and capitalize on opportunities for improvement. It also aims to ensure ongoing hazard identification, risk assessment, and the implementation of necessary controls.

2. SCOPE

The procedure applies to all training and operational activities conducted by ITQAN. All areas of the institute that are covered by the integrated management system (ISO 9001, ISO 14001, and ISO 45001) should adhere to this procedure.

3. RESPONSIBILITY

The responsibility for conducting hazard identification, risk assessment, and defining risk control measures lies with the Management Representative and the Health, Safety, and Environment (HSE) team members. These individuals are tasked with leading the efforts to identify potential hazards, assess risks, and implement appropriate control measures as per the procedure's requirements.

4. DEFINITION

To ensure clarity and consistency in understanding, the procedure provides specific definitions for key terms used throughout the process:

- **Event:** Refers to any exposure to a hazard. This could be an incident or situation where people, property, or the environment may be at risk of harm or damage.
- **Hazard:** Defined as anything with the potential to cause harm. It could be a physical object, a chemical substance, a process, a human behaviour, or any other factor that may pose a threat to health, safety, or the environment.
- **Risk:** The combination of the likelihood of a hazardous event or exposure occurring and the severity of the potential injury, loss, damage, or harm resulting from that event.
- **Incident:** Refers to any adverse event or occurrence that poses a threat to the confidentiality, integrity, or availability of information, systems, networks, or assets.
- **Hazard Identification:** The process of recognizing and acknowledging the existence of a hazard. During this step, the characteristics of the hazard are defined, and relevant information is gathered.
- **Risk Assessment:** Technique used to evaluate not only the likelihood of a hazardous event occurring but also to assess the potential consequences or outcomes, such as injuries, losses, damages, or harms. This evaluation helps in determining the overall risk level associated with a particular hazard.

The implementation of this Hazard Analysis, Risk, and Opportunity Assessment Procedure aims to create a safe work environment by identifying and mitigating potential hazards, incidents, and risks, leading to improved operational performance and better compliance with ISO standards.

5. PROCEDURE

The procedure outlines the steps and guidelines for conducting Hazard Identification and Risk Assessments within the institute. These assessments are aimed at identifying potential hazards/incidents, evaluating associated risks, and implementing appropriate controls to ensure a safe work environment.

5.1. Hazard Identification and Risk Assessment:

Here are the key steps described in the procedure:

- a. Identify various tasks within the process or activity: The first step is to identify the different tasks or activities performed within the institute. This involves understanding the processes and operations that take place.
- b. Identify hazards for the individual tasks: Once the tasks are identified, the next step is to determine potential hazards associated with each task. Hazards can be physical, chemical, biological, ergonomic, psychosocial in nature, or cybersecurity & data breaches.
- c. Assess Risk for the identified hazard: After identifying the hazards, a risk assessment is conducted. This involves evaluating the likelihood of the hazardous event occurring and the potential severity of the consequences.
- d. Identify controls to eliminate, reduce or sustain hazards: Based on the risk assessment, appropriate risk control measures are identified. These measures aim to eliminate or reduce the identified hazards to an acceptable level or sustain the existing controls if they are effective.
- e. Complete the documentation and records: Proper documentation of the hazard identification, risk assessment, and risk control measures is essential. Records of these assessments are maintained for future reference and review.
- f. Implement the risk control measures: The identified risk control measures are implemented to mitigate the identified hazards effectively.
- g. Review the process at least annually or when changes happen: Periodic review of the hazard identification and risk assessment process is necessary to ensure its effectiveness and to account for any changes in operations or activities.
- h. Re-assess for the reduced risk when required: If new control measures are implemented or changes occur in the work environment, it is necessary to re-assess the risks to determine if they have been reduced to an acceptable level.
- i. Further review, identify and implement controls: Continuous improvement is encouraged, and if new hazards are identified or existing controls are found to be inadequate, further reviews and implementations of controls are carried out.

Hazard identification, risk assessment and risk control measures for all the activities undertaken by the Institute are carried out and recorded in Hazard Analysis and Risk Assessment Register (ITQAN/MR/07) in accordance with the steps given in clause 5.1 of this procedure. This

document shall be distributed and explained to all the employees at different levels of the institute, contractors, and other visitors as applicable.

5.2. Hazard Analysis and Risk Assessment Register:

All hazard identification, risk assessments, and risk control measures are documented and recorded in the Hazard Analysis and Risk Assessment Register (ITQAN/MR/07). This document is distributed and explained to all employees, trainees, contractors, and visitors to ensure awareness and understanding of potential hazards and safety measures.

5.3. Inclusivity in Risk Assessments:

The risk assessments consider the safety of employees, trainees, visitors, and anyone else present in the workplace.

5.4. Compliance with Local Authorities:

The institute identifies applicable local authorities' approvals, licenses, and permits required for risk assessments. The relevant management system procedures incorporate local regulatory requirements for risk assessments.

5.5. Hazardous Chemical Substances Transportation:

For the transportation of chemical substances, specific requirements are outlined. The chemical hazards are identified, and risk phrases are assigned to describe the hazards.

5.6. Proportionate Derail of Risk Assessment:

The level and extent of the risk assessment process depend on the level of risk involved. Higher risks require more detailed and comprehensive risk assessments.

Overall, the procedure emphasizes a systematic approach to hazard identification and risk assessment while ensuring compliance with local regulations and promoting a safe workplace for all individuals associated with the institute.

5.7. Identification of hazards:

The procedure focuses on the identification of hazards to ensure a comprehensive and systematic approach to consider all potential risks. The identification of hazards involves examining various sources of information and consulting with relevant parties. Here are the key points highlighted in this section:

- Routine and Non-routine Activities: Hazards can arise from day-to-day operational activities, as well as from non-routine or unplanned situations.
- Short-term and Long-term Activities: Hazards may vary depending on the duration of the activities, and both short-term and long-term activities need to be considered.

- **Reviewing Seriousness and Accident Information:** Past accident data and the seriousness of potential consequences are reviewed to understand the nature of hazards.
- **Human Capabilities and Limitations:** Factors related to human capabilities and limitations are considered, along with interactions between different activities.
- **Information about Tools, Machines, Systems, and Activities:** Information about equipment, machinery, systems, and work processes is considered.
- **Consultation with Employees:** Employees directly involved in the activity or task are consulted to gather their insights and knowledge about potential hazards.
- **Consideration of Surrounding People:** The hazards affecting people in the vicinity of the workplace, such as passersby, contractors, and neighbours, are also evaluated.
- **Hazards Beyond Direct Control:** Hazards that arise in locations not directly under the control of the institute are considered.
- **Hazards Due to Changed Work Process:** Any changes in work processes that may introduce new hazards are taken into consideration.
- **Potential Emergency Situations:** Hazards related to potential emergency situations, such as fires, natural disasters, or civil unrest, are identified.
- **Direct Observation:** Observations of the actual work activities are conducted to understand the real hazards present in the workplace.
- **Changes in Knowledge and Information:** The procedure emphasizes the importance of staying updated with changes in knowledge and information related to hazards.

The identified hazards are categorized into six types based on their nature:

1. **Physical Hazards:** Hazards related to machines, lighting, temperature, height, noise, vibration, pressure, and humidity.
2. **Chemical Hazards:** Hazards associated with solids, liquids, gases, fumes, etc., that have the potential to cause harm to exposed individuals.
3. **Biological Hazards:** Specialized hazards such as Molds, fungus, spores, and diseases (e.g., legionella) are considered.
4. **Ergonomic Hazards:** Hazards related to poor workplace design and the man-machine interface, such as computer workstations, lifting and handling, and slipping and tripping.
5. **Electrical Hazard:** Hazards related to electrical systems, wiring, equipment, and potential exposure to electric shock or fire due to electrical malfunctions or failures.
6. **Information Systems Hazard:** Hazards related to the misuse, malfunction, or compromise of information technology systems, including cybersecurity threats, data breaches, and software vulnerabilities.

By identifying and categorizing these hazards, the institute can take appropriate measures to mitigate risks and ensure the safety and well-being of all individuals involved in the workplace.

5.8. Evaluation of the Risk:

After hazards are identified, the working group evaluates the relative importance of each risk based on their knowledge and experience within the workplace. The evaluation criteria are used to assess the severity of the risk and the likelihood of an incident occurring, considering existing control measures.

The working group assesses each identified hazard by considering the following factors:

- **Severity of Impact:** The potential severity of harm to individuals, institute assets, or data integrity is thoroughly assessed. This analysis spans from minor effects to critical. Understanding the potential impact aids in prioritizing resources and responses effectively.
- **Likelihood of Incident:** The likelihood of an incident occurring when exposed to the specific hazards is determined. This ranges from rare to happen to almost certain to happen.
- **Existing Control Measures:** The effectiveness of existing control measures already in place to reduce the identified risks is considered.

5.9. Documenting Risk Evaluation:

The identified risks are evaluated based on the evaluation criteria provided below, and the results of the evaluation are documented in the Hazard Analysis and Risk Assessment Register ([ITQAN/MR/07](#)).

5.9.1. Severity of Risk:

The severity of risk is expressed in terms of the potential effects on people or property. The following factors affect the severity of effects:

- The number of people who may be affected.
- Individuals particularly at risk due to disabilities or medical conditions.
- Properties of materials, speeds, heights, and weights.
- Amount and type of energy involved.

The severity is classified into five categories:

- 1.Minimal - Not critical and have minimal impact on people or property.
- 2.Minor - Injury requiring First Aid Only, Property loss.
- 3.Moderate - Injury, Illness resulting in temporary disability, Property loss.
- 4.Major - Injury, Illness resulting in permanent disability, Property loss.
- 5.Catastrophic - Death, Property loss.

The severity of risk is expressed in terms of the potential effects on information, systems, and operations. The following factors affect the severity of effects:

- The scope of sensitive information exposed.
- Impact on critical systems and services.
- Regulatory and legal implications.

- Reputational damage.

The severity is classified into five categories:

- 1.Minimal - Not Critical - Limited impact on information and systems & minimal disruption to operations.
- 2.Minor - Limited compromise of non-sensitive information & minor disruption to non-critical systems.
- 3.Moderate - Exposure of sensitive information with moderate impact & disruption to critical but recoverable systems
- 4.Major - Significant exposure of sensitive information & disruption to critical systems with long-term effects.
- 5.Catastrophic (Severe Impact) - Widespread exposure of highly sensitive information & complete disruption of critical systems with irreparable damage.

5.9.2. Likelihood of Risk:

The likelihood of risk is determined based on the worst-case scenario, considering factors such as:

- Number of occurrences of the situation.
- Location of the hazard.
- Duration of exposure.
- Environmental conditions.
- Competence of the people involved.
- Condition of equipment.

The likelihood of risk associated with information, systems, and operations are considering factors such as:

- Historical occurrence of similar incidents.
- Vulnerabilities in systems and applications.
- Effectiveness of security controls.

Likelihood for hazard or incident is also classified into five categories based on frequency:

- Rare to Happen
- Unlikely to Happen
- Possible to Happen
- Likely to Happen
- Almost Certain to Happen

By evaluating risks and incident based on these criteria, the institute can prioritize and focus on addressing the most critical and significant risks first, ensuring effective risk management and improved safety in the workplace.

5.9.3. Risk Rating:

The concept of risk rating, which is used to quantify the level of risk associated with a particular hazard based on the combination of its likelihood and severity. The risk rating provides a numerical value that represents the overall risk level, helping to prioritize risk management efforts. The risk rating is calculated by multiplying the scores assigned to the severity and likelihood of the risk. The resulting rating is then categorized into different risk levels. Here's a breakdown of the process:

5.9.3.1. Likelihood and Severity Scores:

Likelihood and severity are both classified into categories based on the criteria described earlier (e.g., five categories for each). Each category is assigned a numerical score to represent its level. For example:

- Likelihood Score:
 - i. Rare to Happen: 1 (almost impossible)
 - ii. Unlikely to Happen: 2 (could happen but not often)
 - iii. Possible to Happen: 3 (could happen occasionally)
 - iv. Vey Likely to Happen: 4 (probable to occur)
 - v. Almost Certain to Happen: 5 (expected to occur frequently)

- Severity Score:
 - i. Minimal: 1
 - ii. Minor: 2
 - iii. Moderate: 3
 - iv. Major: 4
 - v. Catastrophic: 5

5.9.3.2. Calculating the Risk Rating:

To calculate the risk rating for a specific hazard or incident, the likelihood score and the impact score are multiplied. The resulting value represents the overall risk level associated with that hazard or incident. The range of the risk rating will vary from 1 (representing a low-risk level) to 25 (representing a critical-risk level).

5.9.3.3. Risk Rating Categorization:

The risk rating value obtained is used to categorize the risk into different levels. The specific categorization thresholds may vary depending on the institute's risk assessment criteria. Common risk rating categories include:

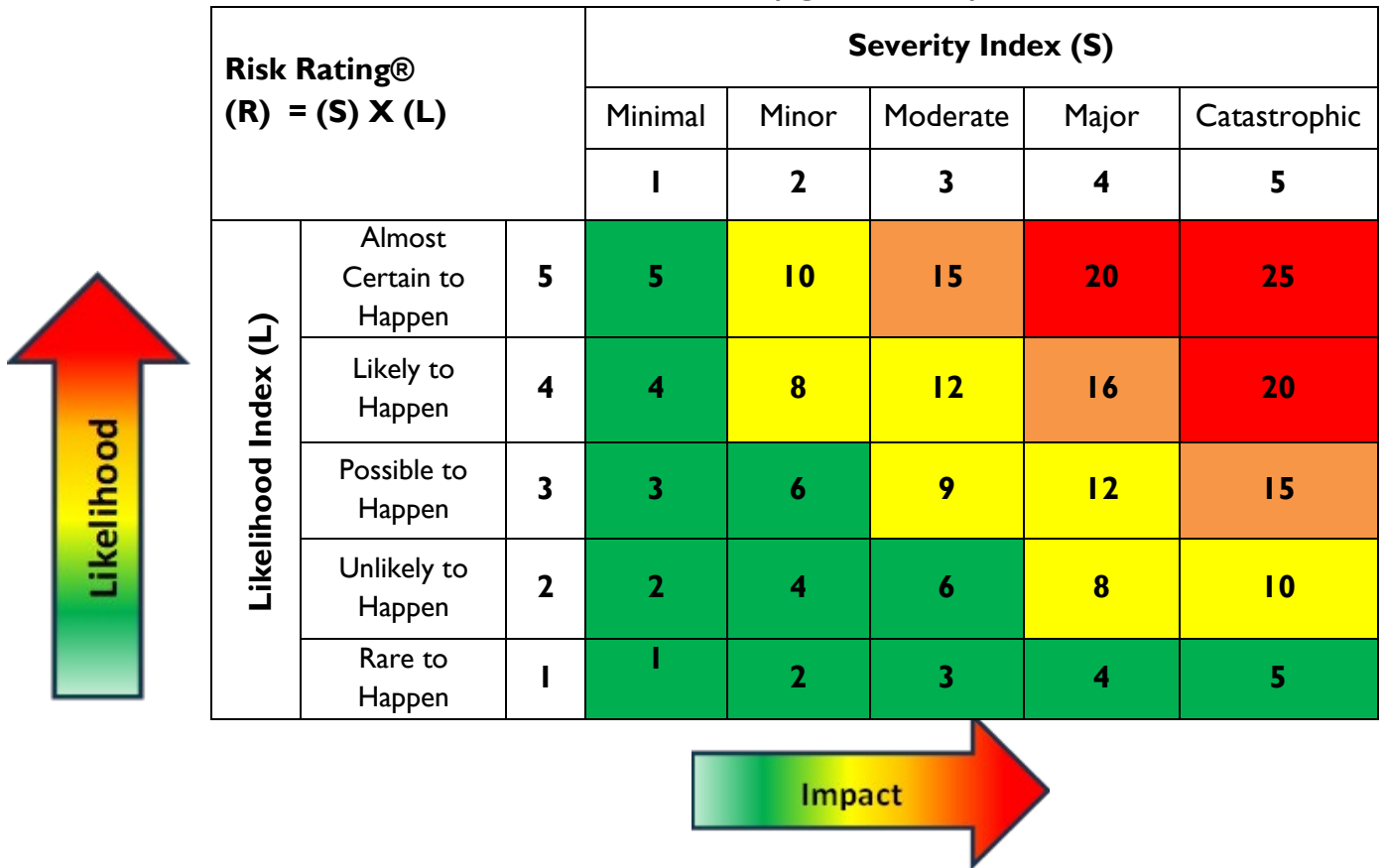
- ❖ Low Risk: Risk rating from 1 to 6
- ❖ Moderate Risk: Risk rating from 7 to 12

- ❖ High Risk: Risk rating from 13 to 16
- ❖ Critical Risk: Risk rating from 17 to 25

By using the risk rating, the institute can quickly identify hazards and incidents that pose the highest risk levels, allowing them to prioritize risk control measures and allocate resources accordingly. This systematic approach to risk assessment and rating helps in making informed decisions to manage and reduce potential risks effectively.

Risk Rating ® = Severity Index (S) X Likelihood Index (L)

RISK MATRIX TABLE (figure 5.9.3.1)



| Risk Rating® (R) = (S) X (L) | | | Severity Index (S) | | | | |
|---------------------------------|--------------------------|---|--------------------|-------|----------|-------|--------------|
| | | | Minimal | Minor | Moderate | Major | Catastrophic |
| | | | 1 | 2 | 3 | 4 | 5 |
| Likelihood Index (L) | Almost Certain to Happen | 5 | 5 | 10 | 15 | 20 | 25 |
| | Likely to Happen | 4 | 4 | 8 | 12 | 16 | 20 |
| | Possible to Happen | 3 | 3 | 6 | 9 | 12 | 15 |
| | Unlikely to Happen | 2 | 2 | 4 | 6 | 8 | 10 |
| | Rare to Happen | 1 | 1 | 2 | 3 | 4 | 5 |

RISK RATING TABLE (figure 5.9.3.2)

| RISK (R = S X L) | DESCRIPTION | ACTION |
|-----------------------------|----------------------|--|
| 1-6 | Low Risk | Risks that are not critical to ITQAN and can be managed without a significant amount of effort |
| 7-12 | Moderate Risk | Risks that require attention but can be managed with some effort |
| 13-16 | High Risk | Risks that are critical to ITQAN and require immediate attention and action |
| 17-25 | Critical Risk | Risks that pose an imminent threat to ITQAN and require urgent action to prevent or mitigate the impact. Activity should NOT be started or continued until the risk is reduced to an acceptable level. |

5.10. Hazard Risk Response Time Objectives (HRRTOs)

ITQAN established Hazard Risk Response Time Objectives (HRRTOs) to determine how to respond promptly and mitigate risks. These HRRTOs range from a few minutes for critical risk to a week for less severe risk:

1. Critical Risk:

- Objective: Respond to and mitigate critical risks that pose an immediate threat to ITQAN Institute's employees, trainees, visitors, contractors/suppliers, assets, property, reputation, or data/information.
- HRRTO: Within 1 minute - 3 hours of detection.

2. High-Priority Risk:

- Objective: Address high-priority risks that have the potential to cause significant harm/damage/interruption but might not require immediate attention.
- HRRTO: Within 3 hours - 8 hours of detection.

3. Moderate-Priority Risk:

- Objective: Handle medium-priority risks that could impact operations, security, or system.
- HRRTO: Within 8 hours - 1 business day of detection.

4. Low-Priority Risk:

- Objective: Manage low-priority risks with minimal impact on operations, security, system.
- HRRTO: Within 1 business day – a week of detection.

5.11. Determination of Controls

The risk control process prioritizes the highest ranked risks and systematically evaluates each risk using the "Hierarchy of Controls." This hierarchy provides a structured approach to determine the

most effective control method for each risk, starting with eliminating the hazard, followed by substitution, engineering controls, administrative controls, and, as a last resort, personal protective equipment (PPE).

- **Eliminate the hazard:** The most effective way to control a risk is to eliminate the hazard entirely from the workplace.
- **Substitute with a lesser hazard:** If elimination is not feasible, consider substituting the hazard with a less harmful alternative.
- **Use engineering controls:** Employ engineering solutions like lockout procedures, process changes, presence-sensing systems, ventilation, or machine guarding to reduce the risk.
- **Administrative controls:** Implement management systems and workplace procedures to minimize risk and promote safety. This should include the use of written procedures to indicate:
 - How tasks are to be undertaken.
 - Who is permitted in the work area.
 - What the requirements for operating different types of equipment are.
 - Operator competencies; and
 - Any training and supervision needed.
- **Personal Protective Equipment (PPE):** Provide appropriate PPE to workers exposed to hazards, but only as a backup support when other control measures are insufficient.
- **Documenting risk control:** The risk control process should be fully documented, and records of risk control measures should be maintained alongside other relevant risk management records.

The use of elimination and substitution controls is more effective in reducing risk because they directly target the hazard. Other controls may only reduce exposure but not the hazard itself.

Considering incidents involving information and system security within the institute, the following hierarchy provides a structured approach to determine the most effective control method for any incident:

- **Detection:** When an incident is detected, the suspicious activity should be flagged within the institute's system logs, indicating the incident occurs to the system or the data.
- **Investigation:** The IT team is to launch an immediate investigation to discover the source of the incident and the effect occurred on the system or the information.
- **Elimination:** The first step should be eliminating the hazard altogether.
- **Replacement:** The team reviewed the system and access control process to prevent such incidents in the future. Replacement of effected devices or data and enhancement of security solution is recommended.
- **Administrative Controls:** The institute should revise its access control policies and procedures.

5.12. Assessing Residual Risk:

Upon implementing the risk control measures, the severity and/or probability of the risk involved will be reduced, leading to a minimized risk level. The remaining risk after implementing all control measures is known as the residual risk. Residual risk is assessed using the Risk Rating Table (5.9.3.1.) and recorded in the Risk Assessment Register ([ITQAN/MR/08](#)). While the severity and probability of the residual risk are assessed, they are not recorded.

5.13. Consideration of Client Safety Requirements and Legal Obligations:

To finalize the Integrated Management Programme ([ITQAN/MR/011](#)), the institute must consider client safety requirements, guidelines, and legal obligations. This ensures that the management program aligns with client expectations and complies with relevant laws and regulations.

By following these steps, the institute can effectively identify and control risks, maintain proper documentation, and ensure compliance with client requirements and legal standards, resulting in a safer and well-managed workplace.

6. ASSOCIATED DOCUMENTS

- Hazard Identification & Risk Assessment Register [\(ITQAN/MR/07\)](#)
- Significant Risk and Opportunity Register [\(ITQAN/MR/08\)](#)
- QHSE-IMS Programme [\(ITQAN/MR/11\)](#)