SECURITY RISKS BETWEEN ANALYSIS AND ASSUMPTIONS

Lieutenant Colonel Carmen-Maria MOISE, PhD
Defence Staff
Irina TĂTARU, PhD
"Carol I" National Defence University, Bucharest

DOI: 10.55535/RMT.2024.4.29

The identification, analysis and management of security risks is a real challenge for any state, especially in the current geostrategic context. All of them belong to the risk management process and cannot be left to assumptions, but require a specialized approach by people with expertise in the field. No developed state can afford to leave security risks to chance, because it can cost its very existence as a sovereign and independent state.

In the current security environment, the lack of a correct risk analysis can lead to a weakening of the administrative capacity to respond to new forms of regional or international security threats. In its absence, the state will not be able to take appropriate measures and will not be able to take the necessary actions to protect its interests in the face of vulnerabilities of any type. A careful and in-depth analysis can facilitate the reduction of exposure to different types of risk, resulting in minimizing the negative effects determined by the possible manifestation of the identified security risks. However, risk identification is only a primordial stage in the complex process of risk management.

Keywords: risk; security environment; risk management; communication services; administrative capacity;

INTRODUCTION

Why Security Risk Management? Security risk management is a topic extensively addressed and debated both in the media and official documents, ranging from Romania's National Defence Strategy to various risk registers within public organizations. At times, it may seem overly discussed or even insignificant. However, we believe otherwise. On the contrary, improperly managed security risks lead to organizational decline and, on a larger scale, to the administrative decline of a country, causing a decrease in credit ratings, economic performance, and, in some cases, creating hard-to-repair security breaches.

Even though this subject is widely discussed, debated, and written about, we question whether these risks are managed scientifically within Romania's public entities or if the process is mostly formalism, relying on opinions and assumptions without a solid scientific foundation. It would be intriguing to determine how much of the approach is based on science versus formalism. It would be a significant challenge and difficult to ascertain.

Public entities collectively form the administrative system of the state – its organism. Administrative capacity can be compared to the body's functioning. Good administrative capacity thus reflects a healthy organism. Just as we strengthen the immune system for colder seasons, enhancing administrative capacity must be a priority for any state seeking to counter threats or vulnerabilities to its security.

But how can this be achieved for security risks? What mechanisms and measures ensure the proper functioning of the risk management process in this context? To answer these questions, we have conducted an analysis of documents from other NATO member states to gain an overview of how they manage security risks. We believe that, by adopting examples already implemented in more developed countries and systematically applying them, an organizational culture in this area can be developed.

RISK ANALYSIS IN MOST IMPORTANT NATIONAL DOCUMENTS

Unsurprisingly, this aspect of administrative capacity of managing risks closely tied to public finance management, is identified as a primary vulnerability in Romania's National Defence Strategy for 2020-2024: *"The capacity of state institutions to evaluate and mitigate the impact of risks and threats is limited by the persistence of vulnerabilities in the allocation and management of public funds, as well as in accessing European funds (including those under the 2021-2027 Multiannual Financial Framework); the regulation and organization of essential sectors such as health and education; the development and implementation of public policies."* (National Defence Strategy, 2020, p. 29). Interestingly, this document acknowledges a limited administrative capacity to manage risks due to these vulnerabilities.

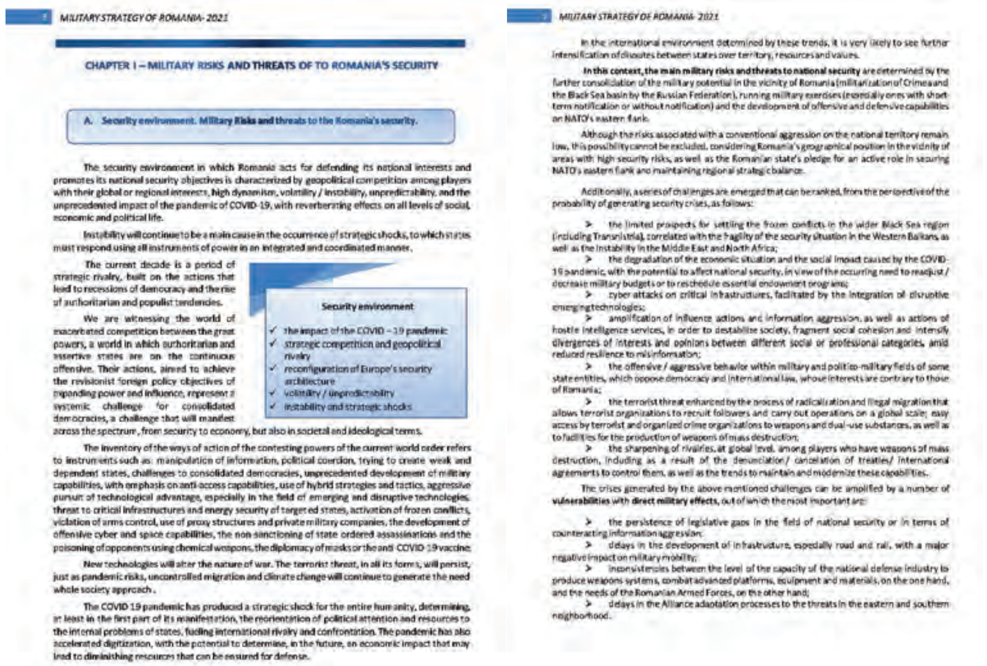
Returning to this aspect, for good risk management, a scientific and professional approach is needed, as well as promptness in determining them. As outlined in the National Defence Strategy for 2020-2024, Romania faces various security risks, including: *"1. The so-called illiberal temptation; 2. The evolution of the Republic of Moldova represents a risk, due to the prospect of counterbalancing the European orientation; 3. The indefinite stagnation of EU enlargement in the Western Balkans; 4. Risks to EU and NATO states from the south; 5. The increasing fragmentation of the international order and the decline of multilateralism; 6. The absence of real multiannual budgetary planning; 7. The persistence of inadequate infrastructure, a deficit in specialized resources, and underfunding; 8. Illegitimate actions undertaken by interest groups; 9. Ongoing dysfunctions in the organization of major public systems (health, education, and social assistance); 10. Intensification of Islamist-jihadist propaganda; 11. The accentuation of demographic decline; 12. Economic challenges, perpetuation of the shadow economy and corruption; 13. Difficulties in managing European funds; 14. The risk of losing cultural heritage; 15. Organized crime groups; 16. Extremist actions; 17. The use of new technologies; 18. Dependence on a limited number of technology providers for communication services; 19. The risk of triggering an interstate armed conflict remains low, but the risk of adapting hybrid offensive operations is looming"*. (Ib., p. 27).

Many of the mentioned aspects can be considered risks according to the theoretical definition, uncertain events likely to occur in the future. However, others are no longer risks, but unresolved problems or manifested risks, which were once in the category of risks, but were not managed well enough to not manifest, such as: *"Persistence of poor infrastructure, shortage of specialized resources and underfunding; Absence of real multiannual budgetary planning; Accentuation of demographic decline".* (Ib.).

According to the same document, Romania also faces additional *"sources of risks"*, which are represented by:

- *"Re-evaluation of arms control regimes, rising defence budgets, and accelerated development of military capabilities by state actors;*
- *Volatility in the security situation in the Western Balkans, along with unresolved conflict hotspots in the broader Black Sea region and limited prospects for resolving frozen conflicts in the region, compounded by a lack of transparency regarding Russian weaponry stationed in the separatist Transnistrian region and prolonged security crises in eastern Ukraine, triggered by the illegal annexation of Crimea;*
- *Phenomena with low probability but with major impact: low-intensity military confrontations, but persistent over time; massive influx of migrants; ecological disasters, natural catastrophes; aggressions against the quality of environmental factors or other calamities."* (Ib.).

Another important national document referencing security risks is the Military Strategy of Romania. We believe that it should address risk management aspects. If significant risks are not included, likely due to public policy decisions we cannot analyse here, such omissions are noteworthy. For instance, in Chapter I – Risks and Military Threats to Romania's Security (Military Strategy of Romania, 2021, p. 7), while the title mentions *"risks"*, no specific risks are described. Instead, the causes that could generate risks and the geopolitical context are described! The latter represent, from a scientific point of view related to risk management, the aspects that must be taken into account in identifying a risk. From the text, we can infer the possibility of a low-probability armed conflict on Romanian territory, but no more than that!



MILITARY STRATEGY OF ROMANIA- 2021

CHAPTER I – MILITARY RISKS AND THREATS OF TO ROMANIA'S SECURITY

A. Security environment. Military Risks and threats to the Romania's security.

The security environment in which Romania acts for defending its national interests and promotes its national security objectives is characterized by geopolitical competition among players with their global or regional interests, high dynamism, volatility / instability, unpredictability, and the unprecedented impact of the pandemic of COVID-19, with reverberating effects on all levels of social, economic and political life.

Instability will continue to be a main cause in the occurrence of strategic shocks, to which states must respond using all instruments of power in an integrated and coordinated manner.

The current decade is a period of strategic rivalry, built on the actions that lead to recessions of democracy and the rise of authoritarian and populist tendencies.

We are witnessing the world of exacerbated competition between the great powers, a world in which authoritarian and assertive states are on the continuous offensive. Their actions, aimed to achieve the revisionist foreign policy objectives of expanding power and influence, represent a systemic challenge for consolidated democracies, a challenge that will manifest across the spectrum, from security to economy, but also in societal and ideological terms.

Security environment

✓ the impact of the COVID – 19 pandemic
✓ strategic competition and geopolitical rivalry
✓ reconfiguration of Europe's security architecture
✓ volatility / unpredictability
✓ instability and strategic shocks

The inventory of the ways of action of the contesting powers of the current world order refers to instruments such as: manipulation of information, political coercion, trying to create weak and dependent states, challenges to consolidated democracies, unprecedented development of military capabilities, with emphasis on anti-access capabilities, use of hybrid strategies and tactics, aggressive pursuit of technological advantage, especially in the field of emerging and disruptive technologies, threat to critical infrastructures and energy security of targeted states, activation of frozen conflicts, violation of arms control, use of proxy structures and private military companies, the development of offensive cyber and space capabilities, the non-sanctioning of state ordered assassinations and the poisoning of opponents using chemical weapons, the diplomacy of masks or the anti COVID 19 vaccine.

New technologies will alter the nature of war. The terrorist threat, in all its forms, will persist, just as pandemic risks, uncontrolled migration and climate change will continue to generate the need whole society approach.

The COVID 19 pandemic has produced a strategic shock for the entire humanity, determining, at least in the first part of its manifestation, the reorientation of political attention and resources to the internal problems of states, fueling international rivalry and confrontation. The pandemic has also accelerated digitization, with the potential to determine, in the future, an economic impact that may lead to diminishing resources that can be ensured for defense.

MILITARY STRATEGY OF ROMANIA- 2021

In the international environment determined by these trends, it is very likely to see further intensification of disputes between states over territory, resources and values.

In this context, the main military risks and threats to national security are determined by the further consolidation of the military potential in the vicinity of Romania (militarization of Crimea and the Black Sea basin by the Russian Federation), running military exercises (especially ones with short-term notification or without notification) and the development of offensive and defensive capabilities on NATO's eastern flank.

Although the risks associated with a conventional aggression on the national territory remain low, this possibility cannot be excluded, considering Romania's geographical position in the vicinity of areas with high security risks, as well as the Romanian state's pledge for an active role in securing NATO's eastern flank and maintaining regional strategic balance.

Additionally, a series of challenges are emerged that can be ranked, from the perspective of the probability of generating security crises, as follows:

➢ the limited prospects for settling the frozen conflicts in the wider Black Sea region (including Transnistria), correlated with the fragility of the security situation in the Western Balkans, as well as the instability in the Middle East and North Africa;
➢ the degradation of the economic situation and the social impact caused by the COVID-19 pandemic, with the potential to affect national security, in view of the occurring need to readjust / decrease military budgets or to reschedule essential endowment programs;
➢ cyber attacks on critical infrastructures, facilitated by the integration of disruptive emerging technologies;
➢ amplification of influence actions and information aggression, as well as actions of hostile intelligence services, in order to destabilise society, fragment social cohesion and intensify divergences of interests and opinions between different social or professional categories, amid reduced resilience to misinformation;
➢ the offensive / aggressive behavior within military and politico-military fields of some state entities, which oppose democracy and international law, whose interests are contrary to those of Romania;
➢ the terrorist threat enhanced by the process of radicalization and illegal migration that allows terrorist organizations to recruit followers and carry out operations on a global scale; easy access by terrorist and organized crime organizations to weapons and dual-use substances, as well as to facilities for the production of weapons of mass destruction;
➢ the sharpening of rivalries, at global level, among players who have weapons of mass destruction, including as a result of the denunciation / cancelation of treaties/ international agreements to control them, as well as the trends to maintain and modernize these capabilities.

The crises generated by the above mentioned challenges can be amplified by a number of **vulnerabilities with direct military effects**, out of which the most important are:

➢ the persistence of legislative gaps in the field of national security or in terms of counteracting information aggression;
➢ delays in the development of infrastructure, especially road and rail, with a major negative impact on military mobility;
➢ inconsistencies between the level of the capacity of the national defense industry to produce weapons systems, combat advanced platforms, equipment and materials, on the one hand, and the needs of the Romanian Armed Forces, on the other hand;
➢ delays in the Alliance adaptation processes to the threats in the eastern and southern neighborhood.

Image 1: Risks and threats of a military nature to Romania's security
(Military Strategy of Romania, ib.)

Continuing with Romania's important documents, we find the *White Paper on Defence*[1], which, according to the Defence Planning Law no. 203/2015, is the departmental-level defence planning document aimed at fulfilling the provisions of the National Defence Strategy and implementing the defence objectives established by the Government Program. The *White Paper* is developed by the Ministry of National Defence, endorsed by the Government of Romania, approved by the Supreme Council of National Defence, and adopted by Parliament, as stipulated by law, for a four-year horizon. In this document, we find, on page 12, the section on Risks and Threats. Upon closer analysis, we can observe that the main risks and threats, as well as their causes, are not clearly delineated. There is mention of the risk of a major conflict, which, in 2021, was categorized as a low-level risk – meaning the probability of such a conflict was considered minimal. We can also deduce the potential occurrence of cyberattacks, identified as possible threats, but there is no identification of potential risks in this area.

[1] Hotărârea nr. 28 din 11 mai 2021 a Parlamentului României, pentru aprobarea *Cartei Albe a Apărării*/Romanian Parliament Decision no. 28 on 11 May 2021 to adopt the *White Paper on Defence*, published in the *Official Gazette of Romania*, Part I, no. 499/13 May 2021.

As we now know, an armed conflict of uncertain duration is currently unfolding near Romania: *"On 24 February 2022, Russia invaded Ukraine, escalating the Russo-Ukrainian war that began in 2014. The invasion, the largest conflict in Europe since World War II, has caused hundreds of thousands of military casualties and tens of thousands of Ukrainian civilian casualties. By 2024, Russian forces occupied approximately 20% of Ukraine's territory. Out of a population of 41 million, about 8 million Ukrainians were internally displaced, and over 8.2 million left the country by April 2023, creating the largest refugee crisis in Europe since World War II"*[2].

In the previously mentioned documents, we observe inconsistencies in the description of risks and cannot identify a clear separation between risks, vulnerabilities, and threats. This simple textual analysis reveals a beginner-level approach to risk management, which, we believe, will not create future opportunities but rather vulnerabilities. This is precisely why we believe it is necessary to develop an organizational culture within public entities, especially in those belonging to the National Security System, that employs advanced risk management practices.

In this context, the examples from other countries that have been utilizing this process for a long time can serve as valuable resources. For illustration, we will mention diverse approaches found in the national documents of the United States of America and the United Kingdom. The snapshots from these documents, identified online, are considered representative and necessary to present for understanding the importance these countries place on risk management.

RISK MANAGEMENT IN DOCUMENTS FROM OTHER NATO MEMBER STATES – USA AND UK

The US National Defense Strategy 2022 (National Defense Strategy, 2022) contains an entire chapter – Chapter IX, page 22 of the introductory section – dedicated to risk management (Risk management/https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF). It highlights the importance of managing all types of risks and acknowledges the possibility of sometimes failing to identify all risks, which could lead to financial efforts being misdirected if risks are not correctly identified. Although not all risks are enumerated (as it is expected since they are the subject of more detailed documents, not the strategy itself), a few key risks are identified that would pose a real danger if intensified. The content emphasizes risks in the areas of cybersecurity and nuclear weapons (Ib.). We also observe the use of specific scientific terms

[2] Invazia Rusiei în Ucraina (2022–prezent)/Russia's invasion of Ukraine (2022-present), https://ro.wikipedia.org/wiki/Invazia_Rusiei_%C3%AEn_Ucraina_(2022%E2%80%93prezent), retrieved on 5 September 2024.

related to risk management, such as *"escalation risk"* (which occurs when a certain threshold is reached, either based on a time interval or another risk condition, thus requiring higher attention – for example, a risk left untreated for more than two fiscal periods might be flagged for additional controls. Another condition might arise if monitoring reveals that the risk exposure rating is expected to significantly exceed initial estimates (https://csrc.nist.gov/glossary/term/risk_escalation) and *"risk mitigation (the prioritization, evaluation, and implementation of appropriate controls/countermeasures recommended in the risk management process to reduce the impact of a risk"* (https://csrc.nist.gov/glossary/term/risk_mitigation*).*

Thus, it can be deduced that a comprehensive analysis was conducted prior to risk identification, and medium- and long-term measures were certainly proposed and outlined for managing these risks.

For a practical example of how risk identification is performed in other countries, we have chosen the United Kingdom model, which we consider very well-applied and organized. In the UK, at the governmental level, there is a public National Risk Register of Security Risks reflecting the National Security Risk Assessment (NSRA) (https://access-national-risk-register.service.cabinetoffice.gov.uk/risk-methodology). Also, on the governmental webpage, we find details on the identification process and can observe the teamwork behind this process.

HOW RISKS ARE IDENTIFIED AND EVALUATED FOR INCLUSION IN THE UK RISK REGISTER

First, risks are identified for inclusion in the NSRA through consultation with a broad range of experts from UK government departments, devolved administrations, the governmental scientific community, and external partners (such as partner agencies, academic institutions, and industry). Impact and probability assessments are conducted by specialized departments for each identified risk within their area of responsibility.

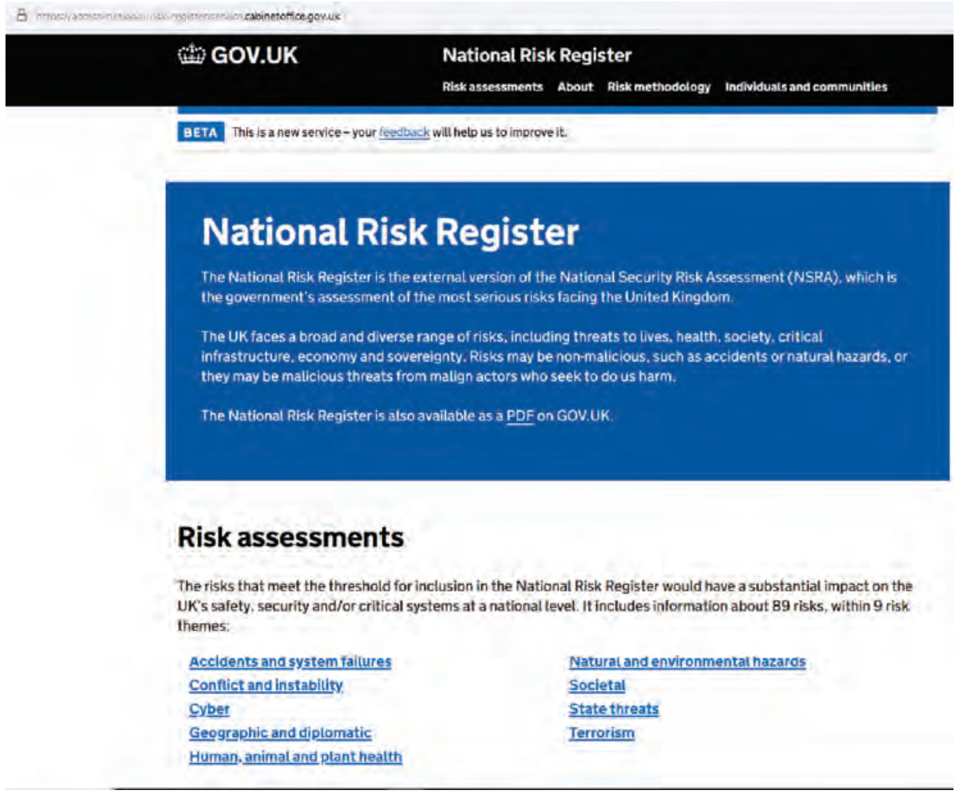
The next step is their classification through evaluation as *"reasonable worst-case scenarios".* These scenarios represent the most incorrect plausible manifestation of a specific risk (once highly unlikely variations are eliminated), enabling specialized entities to engage in proportional planning. Scenarios for each risk were developed in consultation with experts, with data collected from a wide range of sources.

The NSRA does not aim to capture every risk the UK might face. Instead, it seeks to identify a representative range of risks. The National Risk Register (NRR) is the public-facing version, essentially a snapshot of the NSRA, representing the government's assessment of the most severe risks facing the UK.

Not all risks are included in the register, only those that meet a certain *"tolerance threshold",* meaning those that could have a serious impact on the UK's safety, security, and/or critical infrastructures at the national level. The register includes 89 risks across nine risk themes – although many risks could be classified under multiple themes. These themes are: terrorism, cyber risks, state threats, geographic and diplomatic risks, accidents and system failures, natural and environmental risks, human, animal, and plant health risks, societal risks, and conflicts and instability.

The register presents the probability and impact of each risk, following a rigorous and well-tested methodology.

Risks can manifest in various ways, with varying levels of severity. To ensure the UK is prepared for a wide range of scenarios, the NRR establishes a *"reasonable worst-case scenario"* for each risk. It enables planning for all possible scenarios. Additionally, the register includes information on the capacities required for emergency response and recovery methods should a risk materialize.



This is a new service – your feedback will help us to improve it.

National Risk Register

The National Risk Register is the external version of the National Security Risk Assessment (NSRA), which is the government's assessment of the most serious risks facing the United Kingdom.

The UK faces a broad and diverse range of risks, including threats to lives, health, society, critical infrastructure, economy and sovereignty. Risks may be non-malicious, such as accidents or natural hazards, or they may be malicious threats from malign actors who seek to do us harm.

The National Risk Register is also available as a PDF on GOV.UK.

Risk assessments

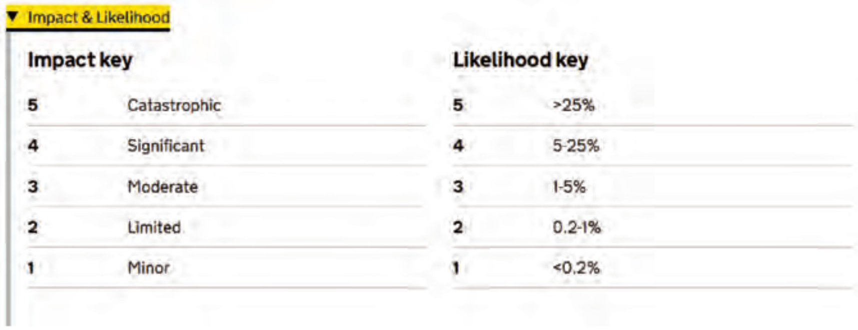
The risks that meet the threshold for inclusion in the National Risk Register would have a substantial impact on the UK's safety, security and/or critical systems at a national level. It includes information about 89 risks, within 9 risk themes:

Accidents and system failures
Conflict and instability
Cyber
Geographic and diplomatic
Human, animal and plant health

Natural and environmental hazards
Societal
State threats
Terrorism

Image 2: The UK National Risk Register
(https://access-national-risk-register.service.cabinetoffice.gov.uk/, retrieved on 9 September 2024)

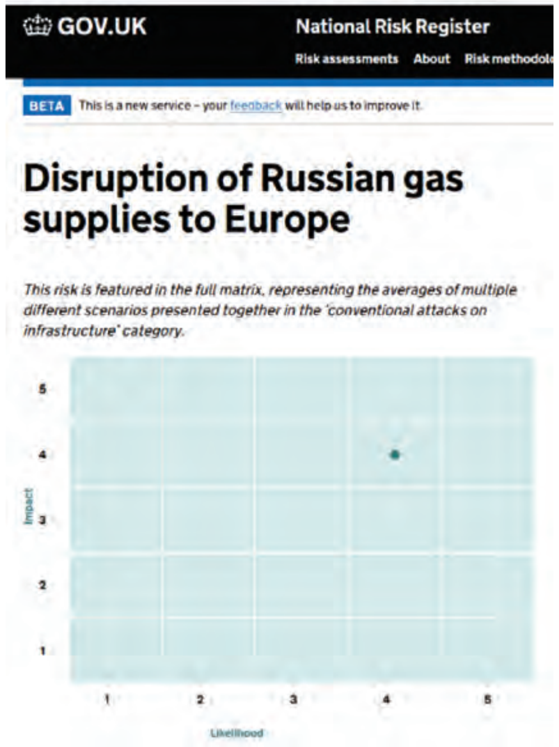
For example, we will present the probability and impact identified for a risk in the register, as well as how to frame the probability and impact according to different possible scenarios, subsequently leading to gradual measures depending on the resulting exposure.



▼ Impact & Likelihood

Impact key		Likelihood key	
5	Catastrophic	5	>25%
4	Significant	4	5-25%
3	Moderate	3	1-5%
2	Limited	2	0.2-1%
1	Minor	1	<0.2%

Image 3: How to determine likelihood and impact
(Geographic and diplomatic, https://access-national-risk-register.service.cabinetoffice.gov.uk/risk-themes/geographic-and-diplomatic, retrieved on 9 September 2024)

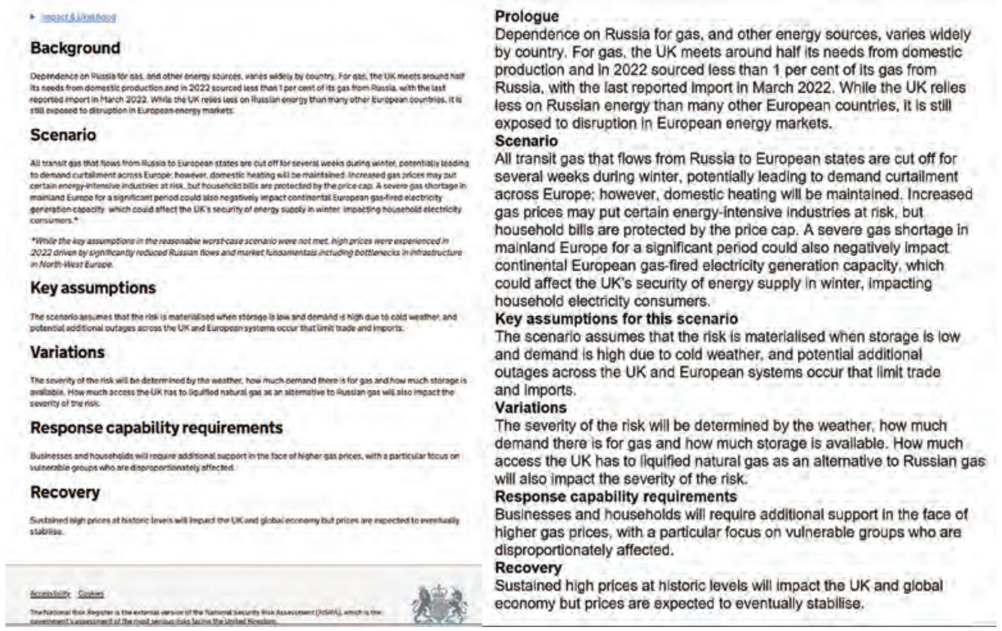


This is a new service – your feedback will help us to improve it.

Disruption of Russian gas supplies to Europe

This risk is featured in the full matrix, representing the averages of multiple different scenarios presented together in the 'conventional attacks on infrastructure' category.

Image 4: Exposure to the risk "Disruption of Russian gas supplies to Europe" presented in the matrix used
(https://access-national-risk-register.service.cabinetoffice.gov.uk, retrieved on 11 September 2024)



▸ Impact & Likelihood

Background

Dependence on Russia for gas, and other energy sources, varies widely by country. For gas, the UK meets around half its needs from domestic production and in 2022 sourced less than 1 per cent of its gas from Russia, with the last reported import in March 2022. While the UK relies less on Russian energy than many other European countries, it is still exposed to disruption in European energy markets.

Scenario

All transit gas that flows from Russia to European states are cut off for several weeks during winter, potentially leading to demand curtailment across Europe; however, domestic heating will be maintained. Increased gas prices may put certain energy-intensive industries at risk, but household bills are protected by the price cap. A severe gas shortage in mainland Europe for a significant period could also negatively impact continental European gas-fired electricity generation capacity, which could affect the UK's security of energy supply in winter, impacting household electricity consumers.*

**While the key assumptions in the reasonable worst-case scenario were not met, high prices were experienced in 2022 driven by significantly reduced Russian flows and market fundamentals including bottlenecks in infrastructure in North-West Europe.*

Key assumptions

The scenario assumes that the risk is materialised when storage is low and demand is high due to cold weather, and potential additional outages across the UK and European systems occur that limit trade and imports.

Variations

The severity of the risk will be determined by the weather, how much demand there is for gas and how much storage is available. How much access the UK has to liquified natural gas as an alternative to Russian gas will also impact the severity of the risk.

Response capability requirements

Businesses and households will require additional support in the face of higher gas prices, with a particular focus on vulnerable groups who are disproportionately affected.

Recovery

Sustained high prices at historic levels will impact the UK and global economy but prices are expected to eventually stabilise.

Accessibility Cookies

The National Risk Register is the external version of the National Security Risk Assessment (NSRA), which is the government's assessment of the most serious risks facing the United Kingdom.

Prologue
Dependence on Russia for gas, and other energy sources, varies widely by country. For gas, the UK meets around half its needs from domestic production and in 2022 sourced less than 1 per cent of its gas from Russia, with the last reported import in March 2022. While the UK relies less on Russian energy than many other European countries, it is still exposed to disruption in European energy markets.
Scenario
All transit gas that flows from Russia to European states are cut off for several weeks during winter, potentially leading to demand curtailment across Europe; however, domestic heating will be maintained. Increased gas prices may put certain energy-intensive industries at risk, but household bills are protected by the price cap. A severe gas shortage in mainland Europe for a significant period could also negatively impact continental European gas-fired electricity generation capacity, which could affect the UK's security of energy supply in winter, impacting household electricity consumers.
Key assumptions for this scenario
The scenario assumes that the risk is materialised when storage is low and demand is high due to cold weather, and potential additional outages across the UK and European systems occur that limit trade and imports.
Variations
The severity of the risk will be determined by the weather, how much demand there is for gas and how much storage is available. How much access the UK has to liquified natural gas as an alternative to Russian gas will also impact the severity of the risk.
Response capability requirements
Businesses and households will require additional support in the face of higher gas prices, with a particular focus on vulnerable groups who are disproportionately affected.
Recovery
Sustained high prices at historic levels will impact the UK and global economy but prices are expected to eventually stabilise.

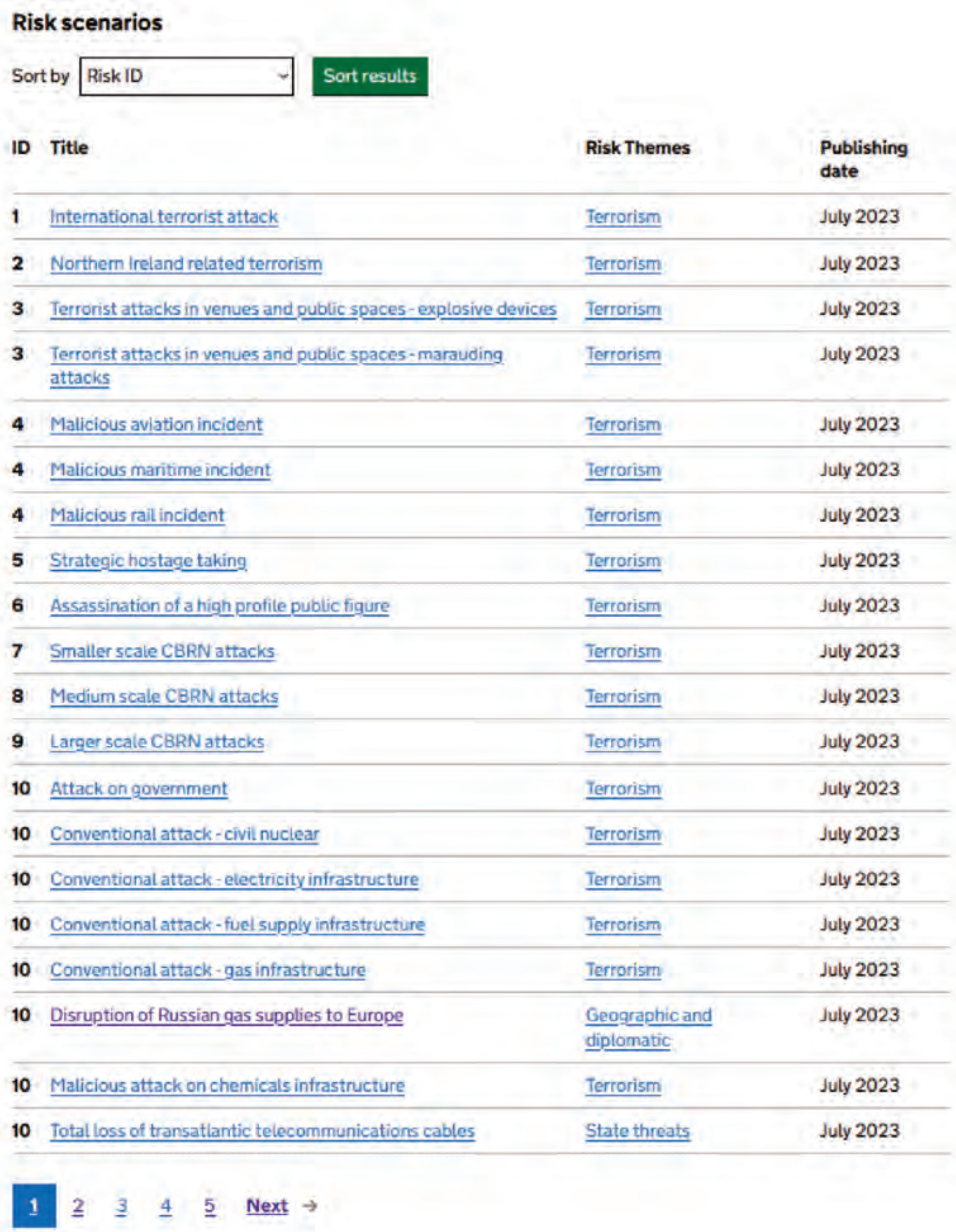
Image 5: Scenario and management of the materialization of the risk in Image 4
(Disruption of Russian gas supplies to Europe, https://access-national-risk-register.service.cabinetoffice.gov.uk, retrieved on 11 September 2024)

In the same platform created for the risk register, we find a grouping of risks identified by themes and a brief description of the management of each risk, depending on a possible scenario, with very easy access to the presentation of each risk, on the page called *"Risk Management"*[3].

IDENTIFICATION, ANALYSIS, AND MANAGEMENT OF SECURITY RISKS – A TRUE CHALLENGE

National security risks must be analysed and managed with the utmost care. It is every state's responsibility to issue coherent public policies that enable the creation of a strong state administration capable of handling various processes, whether simple or complex. Public entities within the national security system must receive increased attention and be allocated the necessary resources to effectively manage security risks. Primarily, human resources make the difference. Competent human resources always add value to any organization; however, they are the most challenging to attract, especially in the current economic context.

[3] *"Risk Management"* page in Risk Assessments (cabinetoffice.gov.uk), retrieved on 11 September 2024.



Risk scenarios

Sort by Risk ID

ID	Title	Risk Themes	Publishing date
1	International terrorist attack	Terrorism	July 2023
2	Northern Ireland related terrorism	Terrorism	July 2023
3	Terrorist attacks in venues and public spaces - explosive devices	Terrorism	July 2023
3	Terrorist attacks in venues and public spaces - marauding attacks	Terrorism	July 2023
4	Malicious aviation incident	Terrorism	July 2023
4	Malicious maritime incident	Terrorism	July 2023
4	Malicious rail incident	Terrorism	July 2023
5	Strategic hostage taking	Terrorism	July 2023
6	Assassination of a high profile public figure	Terrorism	July 2023
7	Smaller scale CBRN attacks	Terrorism	July 2023
8	Medium scale CBRN attacks	Terrorism	July 2023
9	Larger scale CBRN attacks	Terrorism	July 2023
10	Attack on government	Terrorism	July 2023
10	Conventional attack - civil nuclear	Terrorism	July 2023
10	Conventional attack - electricity infrastructure	Terrorism	July 2023
10	Conventional attack - fuel supply infrastructure	Terrorism	July 2023
10	Conventional attack - gas infrastructure	Terrorism	July 2023
10	Disruption of Russian gas supplies to Europe	Geographic and diplomatic	July 2023
10	Malicious attack on chemicals infrastructure	Terrorism	July 2023
10	Total loss of transatlantic telecommunications cables	State threats	July 2023

Image 6: How to access risks by topic and related scenarios

(Risk scenario, https://access-national-risk-register.service.cabinetoffice.gov.uk/risk-assessments, retrieved on 14 September 2024)

The primary goal is to maintain a strong and democratic state. In the risk management process, the correct identification of risks is crucial. We cannot proceed to analyse and manage risks with concrete and coherent measures unless we first succeed in correctly identifying them. According to specialists in the field, risks can be most easily identified through the cause-risk-effect formulation (Mulcahy, 2010, pp. 70-77). To pinpoint the cause(s), several techniques are recommended, the most commonly used being the question: *What if?*

Risk always pertains to the future, which is why it requires information resources, data connections, and complex analyses for accurate identification. Identified risks are not uncovered through revelations or premonitions but through thorough research.

It is also crucial to have constant resources that can be relied upon at any moment for risk identification. The stability of resources is essential; otherwise, the entire risk management process could be jeopardized.

In professional terminology, risks are defined as uncertain events that can positively or negatively impact objectives, projects etc. For this reason, risk management involves minimizing the consequences of negative events (threats) and maximizing the outcomes of potential positive events (opportunities) (Mulcahy, p. 3).

In any case, a risk exists when the percentage of certainty is far below 100% – otherwise, it becomes a fact or a problem, not a risk.

The risk management process itself involves a series of sub-processes. According to Rita Mulcahy, they can be summarized into seven:

1. Establishing institutional rules and policies for risk management or ***Risk Management Planning*** (It entails setting up the type of matrix to be used, defining the structure of the risk register and other necessary documents. Examples of methodologies and document templates can be found in Order no. M.100/ 13 May 2019, issued by the Minister of National Defence, approving the Methodological Norms for the internal managerial control system within the Ministry of National Defence, published in the *Official Gazette* no. 456/6 June 2019). This sub-process encompasses several key activities, illustrated in *Figure 1*:

2. Identification of risks through specific techniques, which we find described in the international standard SR EN 31010/2019 – Risk management. Risk assessment techniques, as well as in the specialized literature. This sub-process entails a series of main activities, presented in *figure 2*.

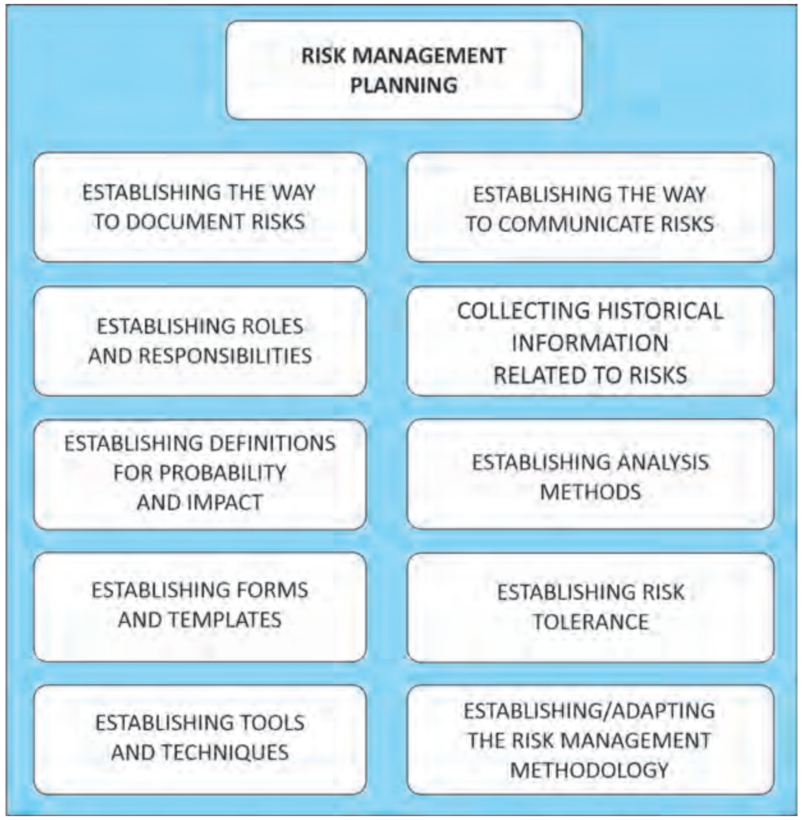

RISK MANAGEMENT PLANNING
ESTABLISHING THE WAY TO DOCUMENT RISKS
ESTABLISHING THE WAY TO COMMUNICATE RISKS
ESTABLISHING ROLES AND RESPONSIBILITIES
COLLECTING HISTORICAL INFORMATION RELATED TO RISKS
ESTABLISHING DEFINITIONS FOR PROBABILITY AND IMPACT
ESTABLISHING ANALYSIS METHODS
ESTABLISHING FORMS AND TEMPLATES
ESTABLISHING RISK TOLERANCE
ESTABLISHING TOOLS AND TECHNIQUES
ESTABLISHING/ADAPTING THE RISK MANAGEMENT METHODOLOGY

Figure 1: Establishing work rules and policies at the institutional level
(authors' design)

3. Qualitative risk analysis which involves establishing a hierarchy of risks based on the estimated level of probability and impact. The main activities of this sub-process would be:

4. Quantitative risk analysis, a sub-process that involves a numerical analysis of the financial impact of risks. The main activities involved would be:

5. Developing the risk response plan, a sub-process that mainly involves establishing coherent and concrete measures to respond to the possible manifestation of risks. The main activities include:

6. Effective implementation of risk response measures, a complex sub-process that involves multiple activities to put into practice the measures established in response with allocated resources. The main activities are:

7. Risk monitoring and risk control, a sub-process that involves maintaining a state of vigilance and carefully monitoring any variations that could change the characteristics of a risk.

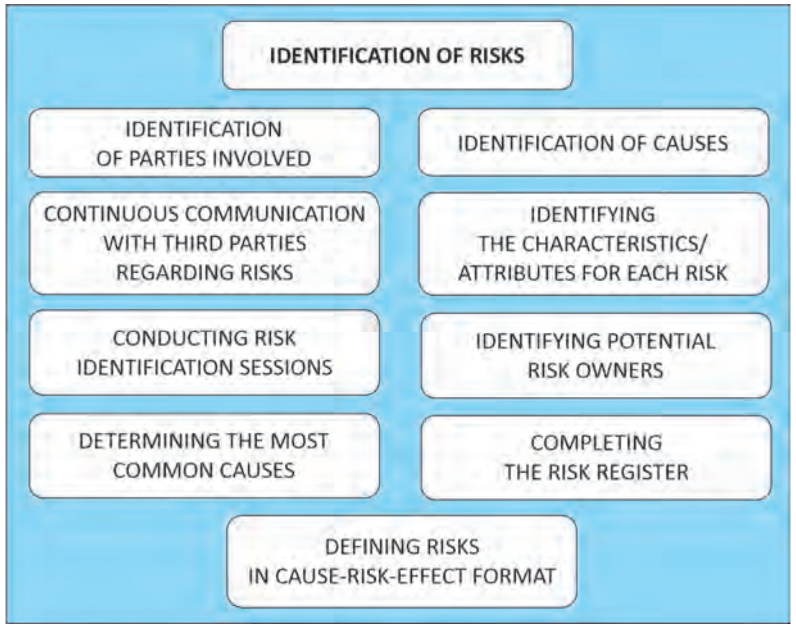

IDENTIFICATION OF RISKS
IDENTIFICATION OF PARTIES INVOLVED
IDENTIFICATION OF CAUSES
CONTINUOUS COMMUNICATION WITH THIRD PARTIES REGARDING RISKS
IDENTIFYING THE CHARACTERISTICS/ ATTRIBUTES FOR EACH RISK
CONDUCTING RISK IDENTIFICATION SESSIONS
IDENTIFYING POTENTIAL RISK OWNERS
DETERMINING THE MOST COMMON CAUSES
COMPLETING THE RISK REGISTER
DEFINING RISKS IN CAUSE-RISK-EFFECT FORMAT

Figure 2: Risk identification (authors' design)

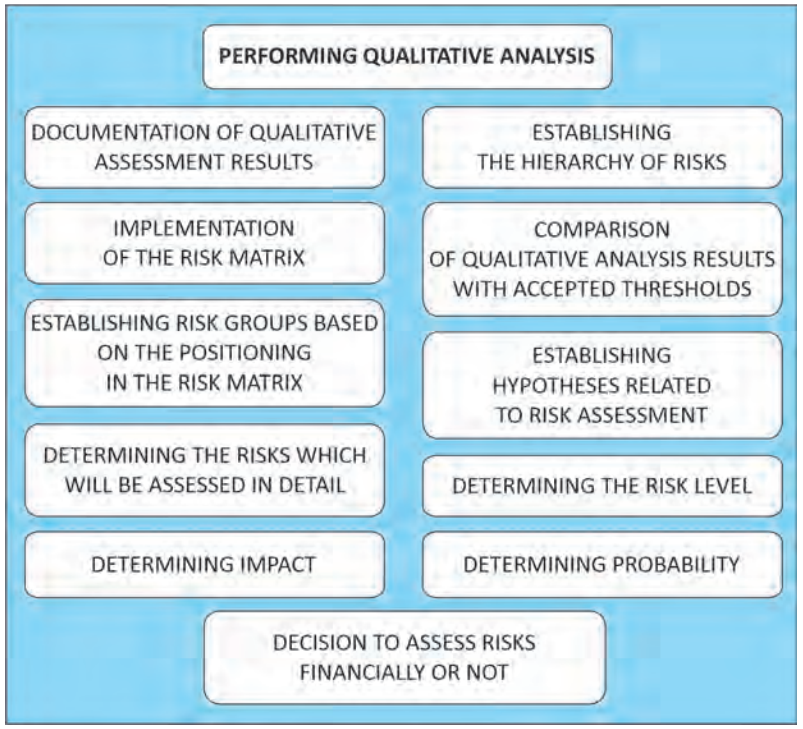

PERFORMING QUALITATIVE ANALYSIS
DOCUMENTATION OF QUALITATIVE ASSESSMENT RESULTS
ESTABLISHING THE HIERARCHY OF RISKS
IMPLEMENTATION OF THE RISK MATRIX
COMPARISON OF QUALITATIVE ANALYSIS RESULTS WITH ACCEPTED THRESHOLDS
ESTABLISHING RISK GROUPS BASED ON THE POSITIONING IN THE RISK MATRIX
ESTABLISHING HYPOTHESES RELATED TO RISK ASSESSMENT
DETERMINING THE RISKS WHICH WILL BE ASSESSED IN DETAIL
DETERMINING THE RISK LEVEL
DETERMINING IMPACT
DETERMINING PROBABILITY
DECISION TO ASSESS RISKS FINANCIALLY OR NOT

Figure 3: Qualitative risk analysis (authors' design)

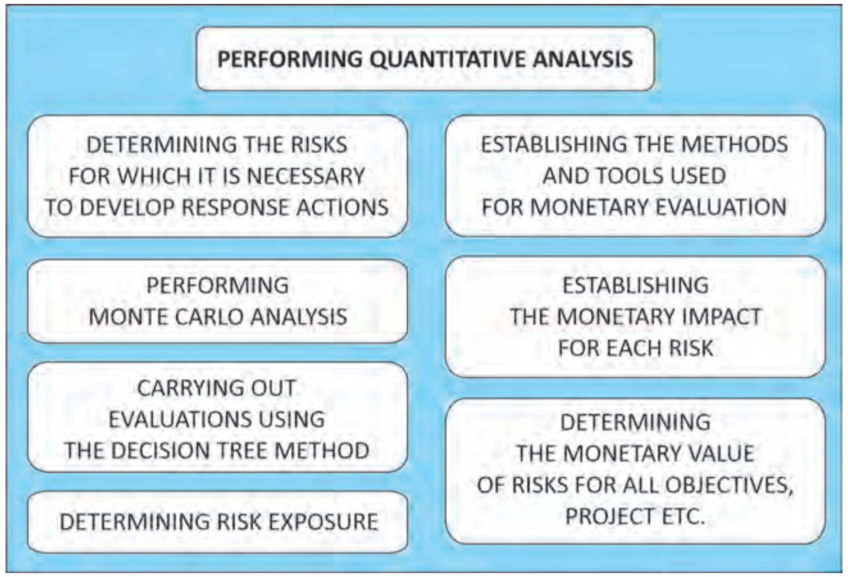

PERFORMING QUANTITATIVE ANALYSIS
DETERMINING THE RISKS FOR WHICH IT IS NECESSARY TO DEVELOP RESPONSE ACTIONS
ESTABLISHING THE METHODS AND TOOLS USED FOR MONETARY EVALUATION
PERFORMING MONTE CARLO ANALYSIS
ESTABLISHING THE MONETARY IMPACT FOR EACH RISK
CARRYING OUT EVALUATIONS USING THE DECISION TREE METHOD
DETERMINING THE MONETARY VALUE OF RISKS FOR ALL OBJECTIVES, PROJECT ETC.
DETERMINING RISK EXPOSURE

Figure 4: Quantitative risk analysis (authors' design)

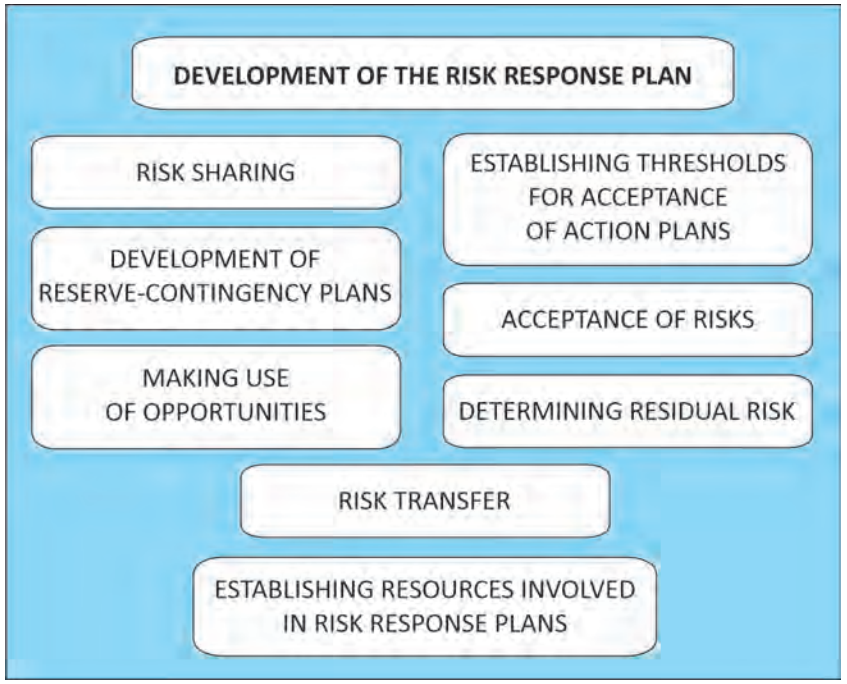

DEVELOPMENT OF THE RISK RESPONSE PLAN
RISK SHARING
ESTABLISHING THRESHOLDS FOR ACCEPTANCE OF ACTION PLANS
DEVELOPMENT OF RESERVE-CONTINGENCY PLANS
ACCEPTANCE OF RISKS
MAKING USE OF OPPORTUNITIES
DETERMINING RESIDUAL RISK
RISK TRANSFER
ESTABLISHING RESOURCES INVOLVED IN RISK RESPONSE PLANS

Figure 5: Developing a risk response plan (authors' design)

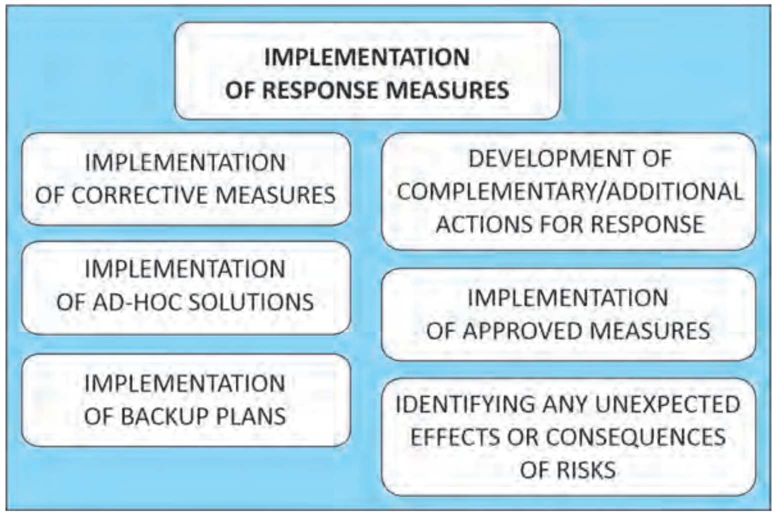

IMPLEMENTATION OF RESPONSE MEASURES
IMPLEMENTATION OF CORRECTIVE MEASURES
DEVELOPMENT OF COMPLEMENTARY/ADDITIONAL ACTIONS FOR RESPONSE
IMPLEMENTATION OF AD-HOC SOLUTIONS
IMPLEMENTATION OF APPROVED MEASURES
IMPLEMENTATION OF BACKUP PLANS
IDENTIFYING ANY UNEXPECTED EFFECTS OR CONSEQUENCES OF RISKS

Figure 6: Effective implementation of risk response measures (authors' design)

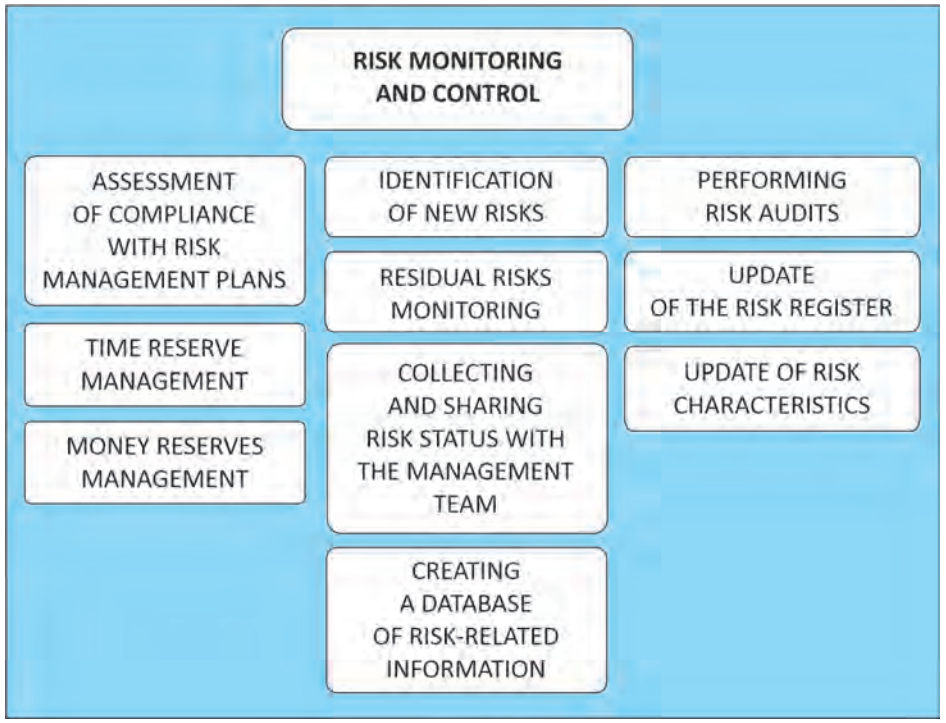

RISK MONITORING AND CONTROL
ASSESSMENT OF COMPLIANCE WITH RISK MANAGEMENT PLANS
IDENTIFICATION OF NEW RISKS
PERFORMING RISK AUDITS
RESIDUAL RISKS MONITORING
UPDATE OF THE RISK REGISTER
TIME RESERVE MANAGEMENT
COLLECTING AND SHARING RISK STATUS WITH THE MANAGEMENT TEAM
UPDATE OF RISK CHARACTERISTICS
MONEY RESERVES MANAGEMENT
CREATING A DATABASE OF RISK-RELATED INFORMATION

Figure 7: Risk monitoring and risk control (authors' design)

Each security risk, once identified, must go through all the necessary sub-processes to be considered and properly managed. Allocating access to multiple types of resources is a real challenge and must be prioritized not only for identifying security risks but also for analysing and managing them. The complexity of this process requires teamwork and constant communication between the actors involved.

CONCLUSIONS

Risk management is the complex process of identifying, evaluating, and managing risks of all kinds, including security risks. Security risks arise from a variety of sources, such as financial uncertainties, technological issues, strategic management errors, accidents, and natural disasters, among others.

The safety of a country lies in its ability to respond to the potential manifestations of identified security risks. For this reason, we believe that continuous preparation through plans, projects, and strategies is a vital necessity for the public administration of any country.

A well-structured risk management program helps to account for the full spectrum of risks a country might face and is implemented in all developed nations around the world. Such programs aid in identifying complex processes that require attention in order to prepare, in advance, the most appropriate response to risks.

Today, more than ever, thanks to the internet, the media, and rapid mobility between states, a risk manifested in one country can easily manifest shortly thereafter in another. For example, risks related to public health issues such as various diseases, or cybersecurity risks. It makes professional risk management all the more necessary and desirable. Risk management is directly influenced by the professionalism of human resources. Human resources should be the **number one priority** of any nation.

The implementation of clear and consistent policies promoting proper risk management is an essential step toward creating a cohesive approach to national security. Establishing and sustaining a risk management culture requires continuous commitment and support. The development of risk management capabilities demands time, resources, training, and ongoing support from top-level managers, adhering to the much-cited principle of the "*Tone of the Top*"[4].

The examples and analyses presented in this text provide a practical demonstration of the necessity and benefits of prioritizing security risk management. Risk management plays a crucial role in achieving the objectives of entities of any kind and aids in identifying risks that may sometimes present opportunities. International standards in the field ensure the use of a universally accepted terminology.

There are numerous benefits to utilizing this process, such as: preparing in advance for potential adverse events and/or opportunities, making well-informed, strategic decisions. Top managers of any organization must constantly take into account potential risks that could impact their established objectives.

The consequences of poor risk management in public administration will directly affect the responsiveness of state entities. These consequences can sometimes be disastrous, leading to the failure of projects, strategies, or actions.

[4] *The first ingredient in a world-class ethics and compliance program Tone at the Top*, https://www2.deloitte.com/us/en/pages/risk/articles/tone-at-the-top-the-first-ingredient-in-a-world-class-ethics-and-compliance-program.html, retrieved on 17 September 2024.

BIBLIOGRAPHICAL RESOURCES:

1. Computer Security Resource Center, https://csrc.nist.gov/glossary/term/risk_escalation, retrieved on 3 September 2024.
2. *Escalation risk*, in Computer Security Resource Center, https://csrc.nist.gov/glossary/term/risk_escalation, retrieved on 3 September 2024.
3. *Hotărârea nr. 28 din 11 mai 2021 a Parlamentului României, pentru aprobarea Cartei Albe a Apărării/Parliament Decision no. 28 on 11 May 2021 to adopt the White Paper on Defence*, published in the Official Gazette of Romania, Part I, no. 499/13 May 2021.
4. *Invazia Rusiei în Ucraina (2022–prezent)/Russia Invasion in Ukraine (2022-present)*, https://ro.wikipedia.org/wiki/Invazia_Rusiei_%C3%AEn_Ucraina_(2022%E2%80%93prezent), retrieved on 5 September 2024.
5. Mulcahy, R. (2010). *Risk Management Tricks of the Trade for Project Managers*.
6. National Defence Strategy 2022, https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF, retrieved on 5 September 2024.
7. *National Risk Register*, https://assets.publishing.service.gov.uk/media/64ca1dfe19f5622669f3c1b1/2023_NATIONAL_RISK_REGISTER_NRR.pdf, retrieved on 6 September 2024.
8. *Risk assessment methodology*, https://access-national-risk-register.service.cabinetoffice.gov.uk/risk-methodology, retrieved on 6 September 2024.
9. *Scenario in the event of a nuclear attack*, https://access-national-risk-register.service.cabinetoffice.gov.uk/risk-scenario/2817, retrieved on 11 September 2024.
10. SR ISO 31000/2018 – *Managementul riscurilor. Principii şi linii directoare*, https://www.asro.ro/a-aparut-sr-iso-31000-managementul-riscului/, retrieved on 11 September 2024.
11. SR EN 31010/2019 – *Managementul riscului. Tehnici de evaluare a riscurilor*, https://www.iso.org/standard/72140.html, retrieved on 12 September 2024.
12. *Strategia Militara a României/Military Strategy of Romania* (2021). București: Ministerul Apărării Naționale.
13. *Strategia Națională de Apărare a Țării pentru perioada 2020-2024/National Defence Strategy* (2020). București: Administrația Prezidențială.
14. https://www2.deloitte.com/us/en/pages/risk/articles/tone-at-the-top-the-first-ingredient-in-a-world-class-ethics-and-compliance-program.html, retrieved on 17 September 2024.