A RISK MANAGEMENT MATRIX FOR ELECTIONS

Developed in the framework of the European Cooperation Network on Elections

Introduction

It is essential to support free, fair and resilient elections, in full respect of fundamental rights and democratic values. Elections have become increasingly complex processes, which require extensive planning and risk management measures, especially in light of the new digital ecosystems.

The integrity and smooth conduct of elections can be influenced by several factors such as the political environment, misuse of digital technologies, insecurity, inaccurate or incomplete information, natural disasters, illicit activities, and the lack of adequate resources for competent authorities.

The sequential timeline of operations, potential large-scale procurement of goods and services, intricate logistical arrangements, extensive processes for staffing the polling stations and training election officials are also critical milestones that elections authorities must achieve to successfully organise free and fair elections. Their successful completion is increasingly more difficult due to the spread of digital technologies and emergence of new players in the information ecosystems.

Continuous risk management supported by predefined criteria for risk acceptance and a standardized methodology is essential to the integrity of elections. Risk management methodologies, such as qualitative and quantitative risk analyses, offer structured approaches for identifying, assessing, and mitigating risks across various contexts, making them well-suited for application in the electoral process. Risk management is a critical component of effective crisis management as it supports, among others, proactive preparedness, the prioritisation of resources and response measures. Robust risk management enhances situational awareness, particularly when it includes real-time monitoring of the election environment to detect threats and address challenges.

Continuous monitoring of the electoral environment is crucial for detecting emerging risks while post-election evaluations provide valuable insights into the effectiveness of risk management strategies and inform improvements for future elections.

This document aims to support Member States in their risk management approach for the conduct of elections. The first step involves identifying potential risks that could affect the election process. Once risks are

identified, they need to be assessed in terms of their likelihood and potential impact. This enables competent authorities to prioritize which risks should be addressed first. Developing strategies to mitigate identified risks is also crucial. This can involve robust planning for logistics, security, and technology, establishing clear frameworks and procedures to address potential challenges, promoting transparency and communication to build public confidence in the electoral process.

The risk management matrix for elections will be regularly reviewed and discussed within the European Cooperation Network on Elections.

Scope

This risk assessment covers different aspects of the election process, including:

- Legal and institutional frameworks relevant for the management of elections,
- Voter and candidate registration,
- Transparency of the electoral process, protection of the information environment and freedom of voters to form their opinion,
- Protection of election-related infrastructure and cybersecurity,
- Data protection,
- Campaign funding,
- The announcement of election results and their review.

Risk categories

The following risk categories are used in this assessment:

1. **Regulatory and institutional risks**: gaps and loopholes in laws and regulations relevant for elections and their enforcement, including election dispute resolution, lack of adequate procedures and protocols for election-related crisis management, inefficient

and unresponsive election-related institutional frameworks and cooperation mechanisms.

2. **Informational and societal risks**: information manipulation and disinformation, including misuse of social media and AI-driven disinformation campaigns.
3. **Physical risks**: risks related to the physical environment, including security, access, and infrastructure, natural disasters and climate-related disruptions of essential services.
4. **Cyber risks**: risks related to the use of technology, including hacking, cyber-attacks, and data breaches.
5. **Operational risks**: risks related to election operations, including voting, counting, and tabulation.
6. **Human risks**: risks related to the people involved in the election process, including voters, candidates, observers, and electoral officials.

Risk identification

Under each category, a catalogue of possible risks has been identified:

Regulatory and institutional risks

1. Gaps and loopholes in election laws and regulations.
2. Gaps in enforcement of laws and regulations relevant for elections, including election dispute resolution.
3. Lack of adequate procedures and protocols for election-related crisis management.
4. Inefficient and/or unresponsive election-related institutional frameworks and cooperation mechanisms

Informational and societal risks

1. Information manipulation and disinformation, including misuse of social media and AI-driven disinformation campaigns.
2. Voter apathy and disengagement.
3. Lack of trust in elections and election authorities.
4. Public incitement to hatred or violence (hate speech), both online and offline.

Physical Risks

1. Unauthorized access to polling stations and counting centres and tampering with ballots and other voting and counting logistics.
2. Disruption of essential services, such as power, water, or transportation.
3. Barriers to accessing voting facilities and materials.

Cyber Risks

1. Hacking or tampering of voting and tabulation information systems.
2. Data breaches.
3. Phishing or malware being introduced into the voting system or electoral infrastructure.
4. Ransomware and wiperware attacks.
5. Distributed Denial-of-Service (DDoS) attacks.
6. Website defacement.
7. Supply chain attacks.
8. Cybersecurity attacks facilitating the creation and spread of manipulated information and disinformation.

Operational Risks

1. Inaccurate or outdated voter data.
2. Lack of access to candidate registration.
3. Coordinated practices affecting negatively the equality of opportunities of political parties and candidates for campaigning.
4. Voting system malfunctioning.
5. Lack of interoperability of different systems
6. Inaccurate or incomplete election results.
7. Delays in the adjudication of election disputes.

Human Risks

1. Voter and/or candidate intimidation.
2. Illegal conduct such as (e.g. bribery, vote buying, trading in influence, misappropriation, illicit political party financing, non-compliance with silence periods etc.).
3. Electoral officials' misconduct, including tampering with votes or manipulating results.

Risk assessment matrix

The following risk assessment matrix is used to evaluate the likelihood and impact of each risk:

Risk	Likelihood	Impact	Risk score
1. Gaps and loopholes in election laws and regulations.			
2. Gaps in enforcement of laws and regulations relevant for elections including election dispute resolution.			
3. Lack of adequate procedures and protocols for election-related crisis management.			
4. Inefficient and/or unresponsive election-related institutional frameworks and cooperation			

mechanisms.			
5. Information manipulation and disinformation, including misuse of social media and AI-driven disinformation campaigns.			
6. Voter apathy and disengagement.			
7. Lack of trust in elections and election authorities.			
8. Public incitement to hatred or violence (hate speech), both online and offline.			
9. Unauthorized access to polling stations and counting centres and tampering with ballots and other voting and counting logistics.			
10. Disruption of essential services, such as power, water, or transportation.			
11. Barriers to accessing voting facilities and materials.			
12. Hacking or tampering of voting and			

tabulation information systems.			
13. Data breaches.			
14. Cyberattacks to the voting system or electoral infrastructure, including phishing or malware being introduced into the voting system			
15. Inaccurate or outdated voter data.			
16. Lack of access to candidate registration.			
17. Coordinated practices affecting negatively the equality of opportunities of political parties and candidates for campaigning.			
18. Voting system malfunctioning.			
19. Lack of interoperability of different systems			
20. Inaccurate or incomplete election results.			
21. Delays in the adjudication of election disputes.			

22. Voter and/or candidate intimidation.			
23. Illegal conduct such as (e.g. bribery, vote buying, trading in influence, misappropriation, illicit political party financing, non-compliance with silence periods etc.).			
24. Electoral officials' misconduct, including tampering with votes or manipulating results.			

Likelihood could be determined by assessing the probability of the risk occurring on a scale from 1 to 5. The categorisation could be based on predictive and/or historical data and expert opinions and should consider the different factors that could influence the occurrence of the risk, such as environmental factors, competence of election officials, resilience of election-related infrastructure, political and economic context.

1. **Minimum Likelihood**: will most likely never occur.
2. **Low Likelihood:** unlikely to occur within the current election cycle.
3. **Medium Likelihood:** could occur once in the current election cycle.
4. **High Likelihood:** likely to occur several times in the current election cycle.
5. **Maximum Likelihood:** certain or almost certain to occur multiple times in the near future.

Impact could be determined based on the extent of what would happen if the risk occurred, notably the effects on election integrity goals, using a scale from 1 to 5. The categorisation could be based on historical data and expert opinions and should consider the different factors that could maximise the impact of the risk, such as complexity of underlying systems, lack of preparedness, over-reliance on specific systems, number of stakeholders.

1. **Minimum impact**: does not affect operations or outcomes.
2. **Low impact:** is easy to manage, with minor disruptions.
3. **Moderate impact:** leads to noticeable disruptions, which can be contained or addressed without major consequences.
4. **Significant impact:** leads to substantial disruptions, requiring a coordinated response and considerable resources to address it.
5. **Severe impact:** major disruptions compromising the entire electoral process.

The risk score could be calculated based on the following formula: Risk score=Likelihood x Impact.

Risk mitigation

The following risk mitigation strategies could be considered:

1. **Gaps and loopholes in election laws and regulations:** Conduct timely post-election evaluations and assessments in the framework of national election networks, with the consultation of relevant law enforcement agencies and civil society, including organisations of election observers.
2. **Gaps in enforcement of laws and regulations relevant for elections:** Conduct regular and transparent evaluations and assessments of the oversight mechanisms and applicable penalties, in the framework of national election networks, with the consultation of relevant law enforcement agencies and civil society, including organisations of election observers.
3. **Lack of adequate procedures and protocols for election-related crisis management:** Conduct timely post-election

evaluations and assessments in the framework of national election networks and identify the needs for early cooperation and preparedness.

4. **Inefficient and unresponsive election-related institutional frameworks and cooperation mechanisms:** Provide regular and transparent activity reports and conduct regular performance audits or peer-review evaluation missions.
5. **Information manipulation and disinformation, including misuse of social media and AI-driven disinformation campaigns:** Implement, in full respect of fundamental rights and democratic values, robust measures and cooperation frameworks to detect, prevent and address swiftly distortion of information on social media, including pre-bunking, debunking. Support fact-checking and civil society organisations with election related expertise; implement voter education initiatives aiming to develop public awareness, media literacy skills and critical thinking. Address situations affecting equal opportunities.
6. **Voter apathy and disengagement:** Implement voter education and civic engagement initiatives.
7. **Lack of trust in elections and election authorities**: Conduct regular public communication activities. Ensure high transparency and accountability of election officials.
8. **Public incitement to hatred or violence (hate speech), both online and offline:** Conduct regular assessments, monitor the election process and implement conflict mitigation measures.
9. **Unauthorized access to polling stations and counting centres and tampering with ballots and other voting and counting logistics:** Implement robust security measures and secure storage of voting and counting materials, including tabulation protocols.
10. **Disruption of essential services, such as power, water, or transportation:** Implement backup power and water supplies, and have contingency plans in place in case of infrastructure failure.
11. **Barriers to accessing voting facilities and materials:** Implement accessible polling stations and voting materials for voters with disabilities.
12. **Hacking or tampering of voting and tabulation information systems:** Implement robust security measures, including firewalls and intrusion detection systems; implement a paper audit trail or a distinct electronic audit trail. Deploy capabilities to ensure a continuity of activities in the event of an incident, including

recovery capabilities. Implement logs, detection mechanisms and efficient network filtering. Improve system robustness to withstand an increase in the volume of requests (denial of service attacks). Ensure the comprehensive application of security updates on the components exposed on the internet (patching policy). Report incidents on the exposed information systems to the cyber security authority without delay.

13. **Data breaches:** Implement robust security measures, including encryption and secure storage of sensitive data.
14. **Cyberattacks to the voting system or electoral infrastructure, including phishing or malware being introduced into the voting system:** Increase cybersecurity awareness, implement robust security measures, including antivirus software and regular software updates. Deploy capabilities to ensure a continuity of activities in the event of an incident, including recovery capabilities. Implement logs, detection mechanisms and efficient network filtering. Improve system robustness to withstand an increase in the volume of requests (denial of service attacks). Ensure the comprehensive application of security updates on the components exposed on the internet (patching policy). Report incidents on the exposed information systems to the cyber security authority without delay.
15. **Inaccurate or outdated voter data:** Implement robust voter registration processes, and mechanisms to cross-check data.
16. **Lack of access to candidate registration**: Provide simple and accessible procedures, facilities and materials, particularly for persons with disabilities.
17. **Coordinated practices affecting negatively the equality of opportunities of political parties and candidates for campaigning:** Implement real-time monitoring measures on equal access to media and online platforms. Apply expeditious sanctions on illegal campaign expenditure and prevent the misuse of administrative resources.
18. **Voting system malfunctioning:** Implement robust quality control measures, including testing and independent certification of voting systems.
19. **Lack of interoperability of different systems:** Conduct regular evaluations and assessments of the interoperability of election-related systems.

20. **Inaccurate or incomplete election results:** Implement robust quality control measures, including manual recounts and verification of vote counts and tabulation.
21. **Delays in the adjudication of election disputes:** Establish clear timelines and provide training and support to adjudicators.
22. **Voter and/or candidate intimidation**: Implement robust measures to prevent voter and candidate intimidation, including notification and complaints mechanisms, dissuasive penalties, voter education and awareness campaigns.
23. **Illegal conduct such as (e.g. bribery, vote buying, trading in influence, misappropriation, illicit political party financing, non-compliance with silence periods etc.):** Implement prevention measures and dissuasive sanctions, codes of conduct, including candidate education and awareness campaigns.
24. **Electoral officials' misconduct, including tampering with votes or manipulating results:** Implement robust selection procedures and integrity criteria, ethical codes of conduct, ethical training and orientation, and dissuasive sanctions.