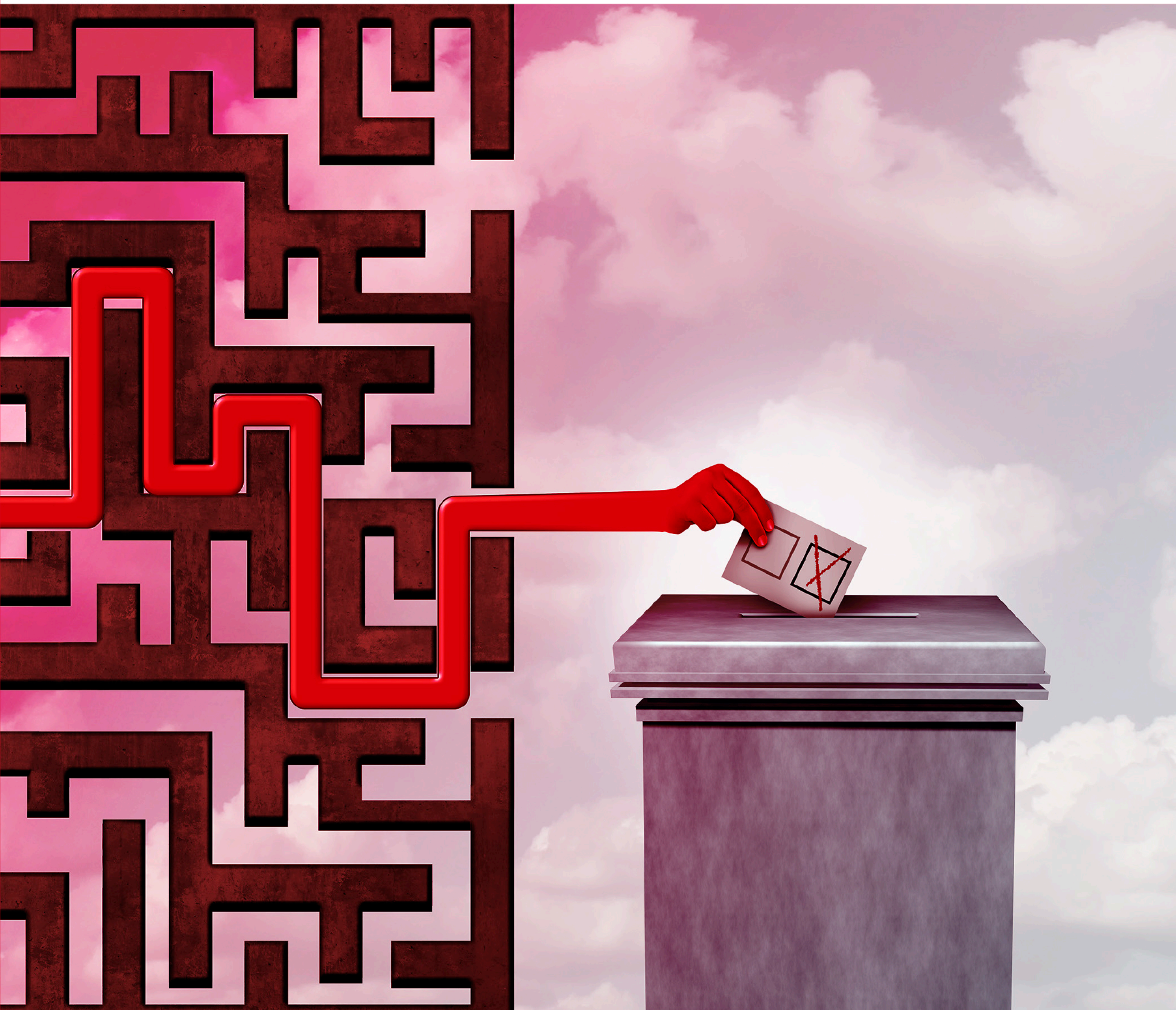
# Risk Management in Elections

## A Guide for Electoral Management Bodies



# Risk Management in Elections

## A Guide for Electoral Management Bodies

Amy Vincent

Sead Alihodžić

Stephen Gale

Our publications are independent of specific national or political interests. Views expressed in this publication do not necessarily represent the views of the Australian Electoral Commission or International IDEA, their Board or Council members.

International IDEA
Strömsborg
SE–103 34 Stockholm
Sweden
Tel: +46 8 698 37 00
Email: info@idea.int
Website: ‹https://www.idea.int›

Australian Electoral Commission
Locked Bag 4007
Canberra ACT 2601
Australia
Tel: +61 (0)2 6271 4411
Website: ‹http://aec.gov.au›

Cover illustration: © Lightwise - Stock Photo - 123RF
Design and layout: KPR

ISBN: 978-91-7671-437-9 (Print)
ISBN: 978-91-7671-438-6 (PDF)
DOI: ‹https://doi.org/10.31752/idea.2021.62›

# Contents

# Acknowledgements

Our thanks go to electoral management bodies that provided insight into their risk management practices through a survey implemented by the Australian Electoral Commission (AEC) and the International Institute for Democracy and Electoral Assistance (International IDEA) in 2019–2020. We also thank the practitioners who shared experiences during the 2018 round table on 'Risk Management in Elections: Strengthening Resilience of Electoral Management Bodies'.

Particular acknowledgement is due to Elections Canada for in-kind contributions to the content and peer review. We also thank the Independent Electoral and Boundaries Commission of Kenya for providing the consultants William Kemboi and Linus Onyango to support the development of case studies and provide comments on an early draft.

Further thanks go to Jeff Pope from the AEC and Therese Pearce Laanela from International IDEA for their initiative, guidance and support in the development of this Guide, and to numerous staff from these two organizations for their support and thoughtful observation at different stages of development. Special mention must be made of the International IDEA interns Fakiha Ahmed, Amna Amin, Niklas Lönn and Beverly Shen for providing support in conducting the survey and analysing the results, and of Jeremy Philp, who was part of the AEC team that contributed to the content and review of the Guide. Finally, we thank Laura Thornton, Director of International IDEA's Global Programmes, and Lisa Hagman, Publications Manager, for their contribution to improving and producing this Guide.

# Preface

Risks to electoral processes impact young and mature democracies alike. Electoral malpractice, foreign interference, disinformation, election-related violence, illicit election funding, insufficient funding and ICT mishaps are examples of risks factors. In cases where these risks have materialized, they have shaken citizens' trust in elections and exposed weaknesses in democratic institutions.

While electoral risks have been palpable and worrisome, the concept of risk management in elections is less well established. A majority of 87 electoral management bodies (EMBs) surveyed by International IDEA in 2014 reported an absence of formal risk management practices. The 2019 comprehensive survey conducted by the Australian Electoral Commission (AEC) and International IDEA confirmed that, where risk management systems existed, they were often limited in scope.

This backdrop explains why the pathbreaking electoral risk management work undertaken by the AEC is so compelling, and why the AEC is taking the topic of risk management so seriously. The AEC manages the conduct of elections in compliance with legislation that is 100 years old, yet electoral processes continue to evolve and face constantly emerging threats and challenges. The AEC continuously evaluates its work and seeks opportunities to collaborate internationally to successfully tackle these risks and threats.

For International IDEA, this Guide builds on a body of work beginning in 2013 with the launch of the Electoral Risk Management Tool (ERM Tool). Drawing on experiences gained through its implementation worldwide and through global consultations conducted on this topic in 2015, International IDEA published a policy paper on risk management in elections in November 2016. Nonetheless, EMBs and international electoral assistance providers continuously underline the importance of, and interest in, a comparative knowledge resource that provides operational guidance on the institutionalization of risk management in elections.

Building on a shared interest in advancing, promoting and supporting the enhanced management of risks in elections, the AEC and International IDEA are proud to present *Risk Management in Elections: A Guide for Electoral Management Bodies*.

Tom Rogers
Electoral Commissioner
Australian Electoral Commission

Kevin Casas-Zamora
Secretary-General
International IDEA

# Introduction

Electoral management bodies (EMBs) encounter numerous risks across all phases of the electoral cycle. They operate in environments that are increasingly complex and volatile and where factors such as technology, demographics, human security, inaccurate or incomplete information and natural calamities, to mention a few, create increasing uncertainty. When risks are not understood and addressed, they can undermine the credibility of the process and the results it yields.

While every EMB needs to engage with risk, each one may have its own approach to doing so. Some EMBs rely on their mainstream management processes and the ingenuity of their people to identify and address risks, while others adopt more formal risk management approaches. The experiences of EMBs (and of organizations in other sectors) show that, when formal risk management processes are successfully implemented, the benefits are profound. Greater risk awareness helps organizations to focus their resources on where they are most needed, thus achieving cost-effectiveness. Formal risk management processes help in keeping track of challenges and remedies applied in previous elections so that similar situations can be avoided in the future and responses further improved.

Trends observed over the last decade indicate that EMBs are increasingly moving from informal to formal risk management processes. A fundamental factor contributing to this shift is that ad hoc risk management is reactive in nature, limiting an EMB's ability to shift resources to respond to emerging priorities in a timely manner. This creates unnecessary workloads and frustrations for staff, can lead to exposures in addressing shared risks, drains resources and can lead to undesirable democratic outcomes with a resultant loss of confidence in the EMB. The movement towards formal risk management practices is accelerated by the fact that governments around the globe are increasingly imposing risk management as a compulsory process across all their agencies, including EMBs.

While it is recognized that risk management plays an essential role in protecting the credibility of elections in the face of internal and external threats, the adoption of formal risk management processes can be complex and may require strategic change management. Organizations with complex management structures mandated to organize high-stakes events in challenging environments, which is often the case with EMBs, require the commitment of senior management to successfully adopt formal risk management processes and a framework that is fit for purpose for the EMB and that helps to build organizational capacity and culture. In many instances, successful risk management processes have been developed incrementally and expanded as they proved their relevance.

The purpose of this Guide is to lay out a set of practical steps for EMBs on how to establish or advance their risk management framework. The Guide's chapters reflect the breadth of key considerations in the implementation process and offer basic resources. It is recognized that electoral systems and the environments in which they operate are diverse. In order to ensure relevance for as many EMBs as possible, the content of the Guide is informed by a combination of:

- the first-hand experiences of the AEC in the implementation of risk management processes;
- the findings of a global survey conducted by the AEC and International IDEA in 2019–2020 on the state of risk management in elections which collected responses from 43 EMBs worldwide;
- the first-hand experiences of International IDEA in developing and supporting the implementation of a practical tool for electoral risk management (International IDEA 2013);
- International IDEA's policy recommendations on the topic (Alihodžić 2016); and
- focused case studies and sample materials provided by the EMBs of Canada and Kenya.

The authors have aligned the Guide with the broader literature on risk management, including international risk management standards and literature on the implementation of risk management processes more specifically. The AEC's approach to implementation of risk management is guided by the Commonwealth Risk Management Policy (Australian Government 2014) and a guide for implementing the Commonwealth Risk Management Policy (Australian Government 2016a) (hereafter 'Commonwealth Guide'). Both documents are aligned with the International Organization for Standardization's (ISO) risk management standard and provide a wealth of universally applicable formulations and practical tips for implementing risk management. Therefore, this Guide consistently references both documents.

## Box 1. Benefits of formal risk management for an EMB

### Australia

The Commonwealth Guide (Australian Government 2016a), adopted by the AEC, lists the universal benefits of risk management, which include:

- improved ability to identify, evaluate and manage threats and opportunities;
- improved accountability and better governance;
- better management of complex and shared risks;
- improved financial management;
- improved organizational performance and resilience;
- confidence to make difficult decisions; and
- decreased potential for unacceptable or undesirable behaviours such as fraud and harassment.

### Kenya

The Independent Electoral and Boundaries Commission's (IEBC) Risk Management Framework (2017b) and the 'Public Sector Risk Management Guide' (unpublished) issued by the National Treasury—both revised in 2020 and awaiting publication—outline the benefits of risk management, which include:

- proactive management;
- increased likelihood of achieving objectives;
- improved awareness of the need to identify and treat risk throughout the organization;
- improved identification of opportunities and threats;
- enhanced compliance with legal and regulatory requirements and international norms;
- improved mandatory and voluntary reporting;
- improved governance;
- improved stakeholder confidence and trust;
- establishment of a reliable basis for decision-making and planning;
- improved control;
- effective allocation and use of resources for risk treatment;
- improved operational effectiveness and efficiency;
- enhanced health and safety performance, as well as environmental protection;
- improved loss prevention and incident management;
- minimization of losses;
- improved organizational learning; and
- improved organizational resilience.

# 1. Establishing a risk management framework

A risk management framework is commonly defined as 'a set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization' (ISO 31000:2009). Its purpose is to assist organizations 'in integrating risk management into significant activities and functions' (ISO 31000:2018). For commonly used terms, see Annex A.

When an EMB executive team decides to start implementing or improving existing risk management processes (details on a risk management process implemented by the AEC can be found in Annex B), the first step is to establish or update its risk management framework. In addition to defining how risks are managed, this is also an opportunity to express the tone and expectations of the process. In practical terms, the development of a risk management framework will be easier if informed by an understanding of its key *attributes* and *components*.

## Key attributes of a risk management framework

The establishment or revision of a risk management framework by an EMB will often require that generic risk management standards and principles be tailored to the EMB's organizational structure and operating environment. When the risk management approach is mandated by the government, it will likely come with guidance for its key attributes. An example is the four *attributes* of a risk management framework emphasized by the Commonwealth Guide (Australian Government 2016a) employed by the AEC. The Commonwealth attributes are broadly applicable, and the annotations below contextualize them in terms of electoral processes.

### It is fit for purpose and tailored to the needs of the entity

Implementation of an EMB's mandate for risk management requires somewhat unique arrangements compared to other state entities. The cascading chronology of electoral events, large-scale procurement of goods and services, complex logistical arrangements and timelines, the recruitment of an external workforce, etc. are some milestones in the electoral exercise that need to cater to the voting rights of the population in a single day. Due to the high political stakes of electoral outcomes, these processes are charged with emotions that can exacerbate social tensions. Therefore, the risk management framework adopted by an EMB may require a degree of originality, sophistication and sensitivity. Although electoral risks are country- and election-specific, it is likely that risk management frameworks adopted by peers in other countries may offer valuable insights to those that embark on the same journey.

### It is well understood, consistently applied and integrated across the entity

EMBs are complex organizations whose structure often comprises country and regional offices. Moreover, EMBs periodically create ad hoc facilities for voter registration, training, logistics, etc., which entails the recruitment and training of a temporary workforce on a large scale. In addition to the core EMB staff, risk management must cover activities implemented by temporary staff and external service providers. They all need to be able to understand plausible risks, recognize impending signs and take action or alert those who need to act. It is the risk management framework that details the processes that ensure that risks are managed systematically as opposed to being ad hoc and uncoordinated, or leaving loopholes.

### It details the required actions for designing, implementing, monitoring and reviewing risk management in the entity

When adopting risk management, EMBs may decide to implement it comprehensively, covering all aspects of its management processes, or through incremental steps focusing on priority areas first (Alihodžić 2016). Also, risk management responsibilities can be assigned to selected or specialized staff. In either case, the risk management framework needs to detail what the risk management process will look like, what the responsibilities will be and how the process will be supervised. Anticipating that the initial process will likely advance over time, an EMB should embed flexibility to adapt to new circumstances.

### It is used by officials in their day-to-day decision-making

The critical juncture in the adoption of a risk management process is an EMB's ability to quickly demonstrate that the process benefits the EMB. For this to happen, the EMB's top leadership and managers must consistently apply risk management perspectives to all decision-making processes. Initially, this may be seen as a burden, in particular if a lot of energy is invested in preparing to face risks that never materialize. However, as these processes become routine, their effectiveness will increase. The risk management framework, therefore, needs to ensure that the process is sustained through periods of both high and low work intensity.

## Box 2. Findings of the 2019–2020 EMB survey on risk management in elections

**EMBs were asked how they managed risks.**

| Options included (multiple selections possible) | Number of responses |
|---|---|
| Through our regular and organic and self-initiated management practices | 30 |
| Through formal risk management processes applied in *some areas* of our work | 12 |
| Through formal risk management processes integrated in *all areas* of our work | 11 |
| Other | 7 |

Whereas all EMBs surveyed acknowledge that they manage electoral risks, the way in which risk management is embedded within each organization differs. The most common arrangement is that EMBs manage risks through regular management practices. The number of EMBs that apply formal risk management to all or only to some areas of their work is significantly lower, as is the number of EMBs indicating other arrangements.

In terms of embedding risk management into regular practices, Mexico's EMB points to its framework of internal control and electoral protocols for continuity of operations that include the risk identification process. In Peru, risk management is integrated into a quality management system, which covers the main electoral activities. The EMBs of Bangladesh, Maldives and Mauritius indicate the importance of assessing risks based on previous elections. In El Salvador, the risk management exercise takes place during the formulation of the general election plan.

Among EMBs that apply formal risk management processes in some areas of their work, Latvia's EMB points to formalized risk management relating to IT security and the security of polling stations implemented in cooperation with national security authorities. Guatemala's EMB implements a formal risk management process with respect to conflict and violence prevention.

Among EMBs that integrate formal risk management processes into all areas of their work, the formal risk management framework used by Canada's EMB distinguishes among corporate, programme, event and project risks, thus allowing the agency to manage risk at all levels. Australia's EMB points out that, although it has a formal documented risk management framework, it also recognizes that much informal/organic risk management is undertaken across the organization. Kenya's EMB has institutionalized enterprise-wide risk management through the implementation of a risk management framework.

## Box 2. Findings of the 2019–2020 EMB survey on risk management in elections (cont.)

In terms of other arrangements, Indonesia's EMB points to a hybrid approach in which risk management standards are embedded in regular management practices. Other EMBs, such as those of Botswana and Namibia, are in the process of institutionalizing their formal risk management practices.

**EMBs were asked about who initiated their management processes.**

| Options included (multiple selections possible) | Number of responses |
|---|---|
| EMB | 25 |
| Government | 5 |
| Both EMB and government | 4 |
| Electoral assistance | 3 |
| Other | 2 |

Decisions to embed risk management in the work of EMBs are mainly the result of internal initiatives. In a small number of cases, the government obliges the EMB to embed risk management. There are instances in which the strengthening of risk management was part of international electoral support.

**EMBs were asked how they developed/obtained their risk management practice.**

| Options included (multiple selections possible) | Number of responses |
|---|---|
| Created (devised) internally | 29 |
| Provided by the government | 13 |
| Acquired from an external organization | 14 |
| Acquired from the ISO | 5 |
| Other | 4 |

In most instances, EMB risk management practice is developed internally. Some EMBs indicate that they followed the guidance of government agencies, such as the National Treasury in the case of South Africa, the Commonwealth Government Risk Policy in the case of Australia, and laws in the case of Croatia. In other instances, internally devised practices were developed with the assistance of external consultants, such as in New Zealand and Sweden, or through collaboration with external partners, such as in the case of Bosnia and Herzegovina, Botswana, Kenya and Namibia, which adopted International IDEA's ERM Tool. Three EMBs—those of Australia, Georgia and South Africa—make specific references to the utilization of ISO standards.

In two instances, Finland and Norway, the government developed the risk management framework. In Norway, the Agency for Public Management and eGovernment provided guidance.

### Box 2. Findings of the 2019–2020 EMB survey on risk management in elections (cont.)

Lesotho, Maldives and Portugal point to the absence of a formal risk management system. Instead, in Lesotho, electoral risk management during an election period is carried out by the Security Committee established by security sector agencies. The Maldives specifies that, after each election, the EMB conducts an internal symposium about the difficulties, risks and obstacles posed by the election. In Portugal, risk management is carried out on a case-by-case basis.

Overall, EMBs should ensure that risk management processes and structures are sustainable (Alihodžić 2016); therefore, it may be more beneficial to start taking small, incremental steps towards full implementation rather than attempting to implement a complete framework for electoral risk management immediately (Frigo and Anderson 2011).

### Box 3. Kenya: institutionalization of risk management

Risk management in the public sector in Kenya is guided by a range of government requirements and other standards which set out eight risk management principles to follow when establishing institutional risk management frameworks.

Following the experiences of the 2007 general elections, which were characterized by post-election violence, the Electoral Commission of Kenya was dismissed. The new Interim Independent Electoral Commission (IIEC), which was a precursor to the IEBC, established the Audit, Risk and Compliance Directorate. However, from 2009 when the IIEC was established, there were no formal risk management practices. Risk management was therefore ad hoc, project- or activity-based and stand-alone (not integrated with other electoral processes).

In 2011 the IEBC began collaborating with International IDEA as part of an effort to strengthen risk management by piloting International IDEA's ERM Tool during the 2013 general elections. Training exercises and stakeholder engagement carried out during the pilot period created a greater understanding of the importance of risk management for EMBs, which led to the IEBC's adoption of the ERM Tool as part of its risk management strategy. From 2015 to 2017 International IDEA supported further customization of the ERM Tool within the IEBC.

Furthermore, with support from the United Nations Development Programme, the IEBC engaged a consultant in February 2017 which undertook a risk maturity assessment of the IEBC. The findings led to the development of a draft risk management framework and risk register, which was validated in a workshop with commissioners, directors and risk champions.

### Box 3. Kenya: institutionalization of risk management (cont.)

Following the approval of the risk management framework, the IEBC later developed a risk management policy, standard operating procedures and reporting tools. The IEBC also established structures whereby risk reports are discussed and escalated, with risk management being a standard agenda item at all IEBC meetings. Risk management has been infused into all IEBC processes and supports decision-making at all levels. An internal audit conducted on risk management returned a positive result.

Looking to the future, the Commission plans to automate its risk management process to make risk identification, evaluation and reporting more efficient.

## Key components of a risk management framework

There is no one-size-fits-all approach to the structure and content of a risk management framework. In practical terms, core components of a risk management framework that each EMB should consider are *formal guiding documentation*, *operationalization* and *culture*. This Guide, therefore, provides normative and practical insights for developing a meaningful risk management framework by building these foundational blocks (see Figure 1). EMBs can adopt these at all levels of maturity on their risk management journey. For more details about what is meant by a maturity assessment, see Annex C.

### Developing formal guiding documentation for risk management

A risk management policy is a form of formal guiding documentation, which usually outlines the EMB's intent and approach in principle to managing risk and is endorsed by senior management. The primary audience of a risk management policy is the permanent employees of the EMB. It is critical that the policy statement match the intent of senior management. Overcommitment can cause a loss of trust if senior leaders are disengaged from the policy and not held accountable for failing to manage risks.

Chapter 2 of the Guide illustrates the principles for developing meaningful guiding documentation for risk management.

### Operationalization of risk management

An effective risk management process is an embedded one. On the surface, it is demonstrated by behaviours such as the consistent use of tools, the registration of risks using standardized forms and the reporting of risks on a regular basis. On a deeper level, healthy risk management behaviour is where risk-taking by all levels of staff is reflective of organizational risk tolerance rather than an individual interpretation on a case-by-case basis. This is particularly important when staff are faced with conflicting situations in a highly compressed time frame, such as polling day or during the ballot count after the close of polling. The better defined risky behaviour is, the more confidence senior executives have that employees will use good judgement in making the right call and avoid excessive risk taking where it is not allowed.

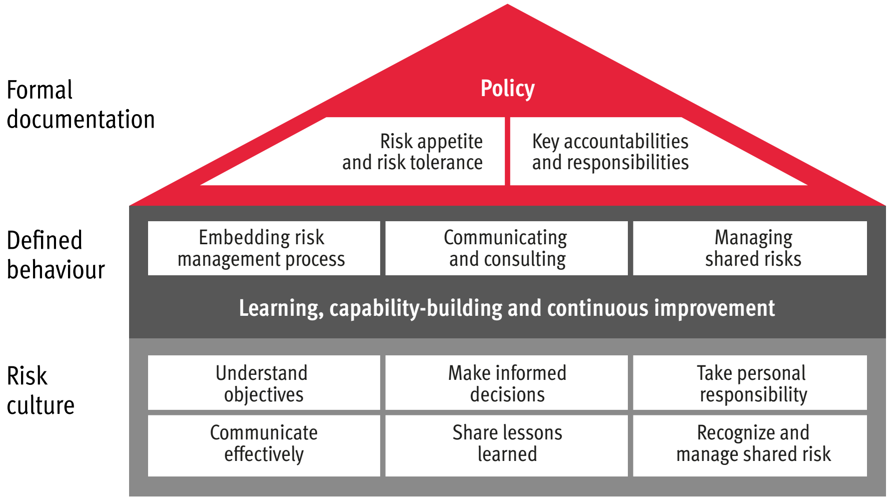
Chapter 3 of the Guide illustrates the operationalization of risk management processes through defined behaviour.

### Building a positive risk management culture and capability

The operationalization of risk management can never be truly successful without a supporting culture. A positive risk culture injects energy and enables the longevity of healthy risk management behaviours. It is often a good idea to conduct a risk culture survey before an EMB embarks on the journey to set up a formal risk management framework. Such a survey usually highlights discrepancies between internal policies and behaviours, capability gaps and existing cultural traits. This can inform the areas of focus and a pathway for improvement.

Chapter 4 of the Guide covers both the positive and negative characteristics of risk culture and provides insights into capability-building.

Figure 1. Risk management framework adopted by the AEC


Formal documentation
Policy
Risk appetite and risk tolerance
Key accountabilities and responsibilities
Defined behaviour
Embedding risk management process
Communicating and consulting
Managing shared risks
Learning, capability-building and continuous improvement
Risk culture
Understand objectives
Make informed decisions
Take personal responsibility
Communicate effectively
Share lessons learned
Recognize and manage shared risk

*Source:* Based on Australian Government, Department of Finance, 'Implementing the Commonwealth Risk Management Policy—Guidance', 2016, <https://www.finance.gov.au/sites/default/files/2019-11/implementing-the-rm-policy.pdf>, accessed 22 April 2021.

## Box 4. Findings of the 2019–2020 EMB survey on risk management in elections

**EMBs were asked about common components of their EMB risk management frameworks.**

| Options provided (multiple selections possible) | Number of responses |
|---|---|
| A register that records risks | 29 |
| Tools to evaluate and assess risks | 27 |
| Risk identification procedure | 27 |
| Risk analysis method | 25 |
| Risk communication procedure | 22 |
| A documented risk policy | 20 |
| Allocation of resources | 20 |
| Tools to treat risks | 19 |
| Risk training materials | 15 |
| Appropriate authority, responsibility and accountability for risk management | 14 |

When responding to survey questions, several EMBs admitted that they lacked a number of elements that they recognized as important. For example, the EMBs of Botswana, El Salvador and Nepal find a documented risk policy important, even though their respective systems lack such a policy. Indonesia's EMB highlights the benefits of having appropriate authority and accountability—elements missing from its risk management practice. The EMBs of Australia and Canada indicate that all elements are present in their risk management systems. In the former, they are at varying levels of maturity, as the EMB continues to embed risk management in its culture.

# 2. Developing formal guiding documentation for risk management

Formal guiding documentation, such as a risk management policy, usually outlines an EMB's intent and approach in principle to risk management in order to guide decision-making and operations. The policy must match the intent of senior management and be clear to the primary audience, which is the permanent employees of the EMB.

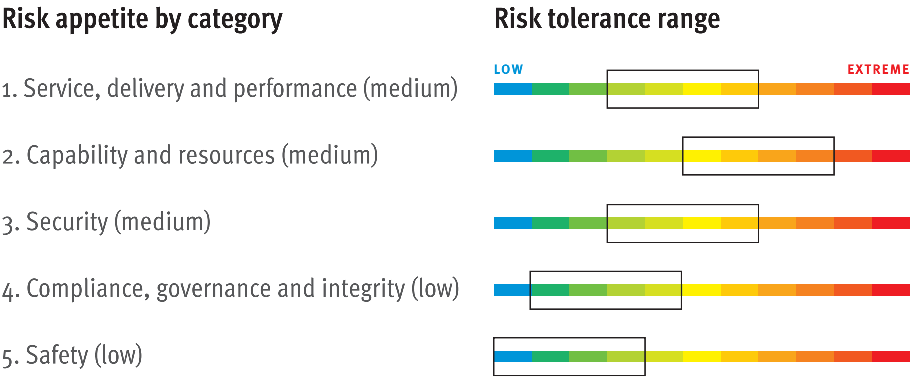
The ISO 31000 (2018: 6–7) states in its risk management guidelines that:

> Top management and oversight bodies, where applicable, should demonstrate and articulate their continual commitment to risk management through a policy, a statement or other forms that clearly convey an organization's objectives and commitment to risk management. The commitment should include, but is not limited to:
>
> - the organization's purpose for managing risk and links to its objectives and other policies;
> - reinforcing the need to integrate risk management into the overall culture of the organization;
> - leading the integration of risk management into core business activities and decision-making;
> - authorities, responsibilities and accountabilities;
> - making the necessary resources available;
> - the way in which conflicting objectives are dealt with;
> - measurement and reporting within the organization's performance indicators;
> - review and improvement.

Australia's Commonwealth Risk Management Policy (Australian Government 2014), to which the AEC aligns its risk management approach, is broadly consistent with the ISO 31000 (2018) guidelines. It advises that a risk management policy be linked to other risk management framework elements through procedures and guidance material. In addition, the Australian Government policy also suggests that a risk management policy should include a visionary statement about what the entity is seeking to achieve through good risk management and key goals for the risk management programme in the future. Moreover, Australian Government agencies are required to ensure that their risk management policy define the risk appetite and risk tolerance of the respective agency, whereby:

- **Risk appetite** is the amount of risk an entity is willing to accept or retain in order to achieve its objectives. It is a statement or series of statements that describe the entity's attitude towards risk-taking. For example, an EMB may have different appetites concerning risks relating to the safety of its equipment and the safety of its people.
- **Risk tolerance** is the specific level of risk-taking that is acceptable in order to achieve a specific objective or manage a category of risk. Risk tolerance represents the practical application of risk appetite and will be most effective when it is easily understood by all officials. For example, the range of risk tolerance is commonly presented on a scale of low, medium and high or from low to extreme, or similar.

### Figure 2. The AEC's risk appetite and tolerance



*Source:* Australian Electoral Commission, excerpt from AEC Risk Appetite and Tolerance Statement, internal document.

Incorporating risk appetite and risk tolerance considerations into an EMB's formal risk management documentation is useful, as it provides an objective way for the EMB's leaders to articulate what constitutes acceptable risk-taking both in their day-to-day work and in achieving the EMB's strategic objectives. Risk appetite and risk tolerance statements provide guidance to staff on how much risk the EMB is prepared to take, areas where it is appropriate to take more or less risk and the constraints on risk-taking.

In practical terms, the AEC establishes risk appetites for five different categories using a scale of low, medium, high and extreme (see Figure 2). Then the risk tolerance range is determined for each category. In areas where an EMB's risk appetite is lower, decisions on managing those risks should consider more mitigation strategies, which will require more resources. On the other hand, in categories where the EMB has a greater risk appetite, there is a general willingness to take on more risk in return for a greater benefit. As a general rule, the materialization of such risks should not jeopardize important EMB objectives, while the potential successes should be of great significance for the organization. A clear articulation of risk appetite and tolerance, therefore, helps officials to both mitigate threats and take advantage of opportunities.

## Box 5. Revision of the AEC's risk management policy

The AEC's risk management policy is a core component of its risk framework, which determines the AEC's:

- approach to risk management;
- framework for risk management (governance and culture);
- risk appetite and risk tolerance;
- commitment to developing its capabilities; and
- roles and responsibilities.

The risk management policy is reviewed approximately every two years. A number of factors informed the scope of the last review, which was published in 2019. These included an organizational restructure, a risk culture review and the results of an annual risk management benchmarking survey in which Australian Government agencies receive feedback on how to improve their risk management frameworks.

The review and the survey results highlighted a number of consistent themes on how the AEC could improve its risk culture and framework, including training and support, incorporating and aligning risk management into agency planning and reporting arrangements, and creating an alignment between agency strategies and risk appetite.

In response, the AEC's risk management policy was updated to include a commitment to developing capability, which includes arrangements for job training, facilitated workshops and online learning modules. The practical implementation of this commitment was a series of training sessions delivered across national and state/territory offices. The work to review the AEC's risk management policy was led by the Risk Unit, with the policy and associated risk appetite statement and risk matrix endorsed by the Electoral Commissioner. In addition, the Deputy Electoral Commissioner communicated the results to the agency to ensure staff awareness and to impart the importance of the policy changes.

### Box 5. Revision of the AEC's risk management policy (cont.)

To ensure that risk management is effectively incorporated into planning and reporting arrangements, the AEC's strategic and enterprise risks are now included in the AEC's corporate plan, which sets out the high-level direction of the agency. In addition, operational business plans include a reference to agency risks so that there is a clear link between operational objectives and risk.

The AEC also developed its first risk appetite statement, which formally articulates acceptable levels of risk-taking within different categories of risk—for example, service delivery, safety and compliance. This directly informs the agency's risk matrix, which is used to assess and evaluate risks (see the AEC's risk matrix and escalation table in Annex D).

There are a range of supporting documents to assist staff in meeting their responsibilities for managing risk, including risk management guidelines and internal case studies on good risk management practice.

### Box 6. Revision of the risk management policy in Kenya

The IEBC sets forth in its risk management policy its overall intentions regarding risk management and provides a framework to ensure that risk management processes are applied consistently across the organization and that they provide reasonable assurance regarding the achievement of the organization's objectives. The policy provides the rationale for risk management, the responsibilities and accountabilities for managing risks as well as the way in which risk management will be monitored and reported as an integral part of the governance structure.

The IEBC's risk management policy is reviewed annually. The review is informed by a post-election evaluation, a strategic plan, and changes to the IEBC's policies.

The last review of the risk management framework and policy was intended to have been effected in early 2020 but was postponed following the outbreak of the coronavirus pandemic. The revision of the documents was finalized and approved by the IEBC in October 2020. In the revised policy, the IEBC established a County Risk Management Committee in each of Kenya's 47 counties.

# 3. Operationalization of risk management

Operationalization of risk management is sometimes referred to as integrating risk management into operations. In practice, this is the hardest part of implementing a formal risk management framework. It requires effort at all levels of the organization covering end-to-end business processes. That is why risk management is everyone's business. All aspects of the guiding documentation must come alive and be integrated into the planning, governing, decision-making and communications strategies. Achieving this takes a concerted effort and deliberation. Furthermore, the reward for this effort is not immediately obvious, and even when it happens, it is often not seen as a result of good risk management unless a targeted review and analysis is undertaken.

## Defining risk management responsibilities

Risk management responsibilities may differ from one EMB to another, reflecting specific organizations' structures, the nature of the risks faced and the approaches taken to embed risk management.

However, responsibility for risk management lies first and foremost at the corporate level. Beyond defining risk management policies, an EMB's leadership needs to include risk considerations in its day-to-day decision-making processes. The process of risk identification, risk monitoring and evaluation, reporting and oversight should be delegated to the lower programme and project management lines.

The ISO 31000 (2018: 7) underscores that top management should ensure that risk management authorities, responsibilities and accountabilities are assigned and communicated at all levels of the organization to:

- emphasize that risk management is a core responsibility; and
- identify individuals who have the accountability and authority to manage risk.

In this respect, an EMB should consider whether accountability and responsibility are designated to individual departments or specialized staff. Central arrangements (such as a Chief Risk Officer, risk unit or cross-functional committee that coordinates risk management efforts across the organization) are considered superior, as they can be assigned with a clear responsibility to drive the improvement of risk management throughout the organization. Typically, a central risk function contains dedicated resources to design, implement and review the risk management framework. Additionally, this central function can also facilitate risk reporting and analysis to help inform the EMB's senior management.

The Commonwealth Guide (Australian Government 2016a) stresses that the responsibility to design, publish and review an organizational risk management framework will be most effective when assigned to a specific person or team. Responsibility for managing individual risks may include the following:

- **Risk owners** who are accountable for managing a particular risk, such as an EMB manager working towards a specific objective—such as voter information—that may be affected by a specific risk (e.g. a misinformation campaign).
- **Control owners** responsible for maintaining the effectiveness of measures to modify risk, such as a person who monitors and reviews specific risks, ensures that control measures are in place and provides oversight. In the case of misinformation, this function can include an analyst.
- **Risk treatment owners** responsible for implementing strategies in cases where the risk level is unacceptable after controls are applied. They may include senior EMB managers who can ensure broader institutional responses to the risks that materialize.

Whatever the arrangement is, an EMB's leadership needs to ensure that sufficient resources are put in place to support this work.

## Box 7. Findings of the 2019–2020 EMB survey on risk management in elections

**EMBs were asked about who had the responsibility to implement their risk management system/practice.**

| Options provided (multiple selections possible) | Number of responses |
|---|---|
| A unit that has a primary or sole risk management (coordination) responsibility | 5 |
| A unit that has another main responsibility but takes charge of risk management and coordination | 14 |
| All units equally, coordinated through regular management processes | 21 |
| All units equally, but not coordinated through regular management processes | 7 |
| Other | 3 |

## Box 7. Findings of the 2019–2020 EMB survey on risk management in elections (cont.)

The responsibility for implementing risk management practices can vary between EMBs. Costa Rica, Kenya and Libya are examples of countries whose EMBs have a unit with the primary or sole responsibility for risk management. In Lesotho, all units are equally responsible for risk management, and they are coordinated through regular management processes.

Among EMBs that have a unit with another main responsibility, those of Croatia and South Africa assign risk management to the Chief of Staff. In Australia, risk management is undertaken by a team which is also responsible for internal audit, assurance and business continuity management. In Malawi, the audit department is in charge of risk management. Botswana's EMB has assigned this responsibility to its Performance Improvement Coordination Unit. In Moldova, the Head of Analysis is in charge.

The most common arrangement for EMBs is one where all units are equally responsible and coordinated through regular management processes (e.g. Lesotho, Zanzibar and Zimbabwe). In Haiti, 'the implementation of the risk management system is the responsibility of the directorates under the leadership of an executive director with the guidance of a board of directors'.

## Box 8. Findings of the 2019–2020 EMB survey on risk management in elections

**EMBs were asked about who owned the electoral risks they face.**

| Options provided (multiple selections possible) | Number of responses |
|---|---|
| Project managers within our organization | 8 |
| Managers who have dedicated elections-related operational roles within our organization | 24 |
| Senior managers within our organization | 25 |
| Ownership is shared with other state agencies | 10 |
| Other | 5 |

The responsibilities for overseeing electoral risks are divided across EMBs. Most commonly, the responsibility lies with the senior managers and managers who have dedicated elections-related operational roles. In some instances, ownership is shared with other state agencies.

In Costa Rica, 'Each electoral program, with specific functions within the process, sends its risk assessment through the respective plans, to the Department of Electoral Programs. This unit validates and consolidates them, and then forwards it to the Directorate of the Electoral Registry, within the Implementation Plan of the Electoral Programs. Management must upload that plan for the approval of the Supreme Electoral Tribunal (TSE).' In Mongolia, all EMB staff regularly inform their supervisors about possible risks that fall within the scope of their responsibilities. In Canada, senior executives take the lead for corporate, programme and event risks, while project managers oversee risk management for their projects.

### Box 8. Findings of the 2019–2020 EMB survey on risk management in elections (cont.)

Australia and New Zealand share similar approaches, choosing all four of the options provided in the survey. In Australia, 'when risks are identified, the appropriate owner of that risk is also identified. Based upon an assessment of that risk, appropriate monitoring and reporting is undertaken. Third-party risks may be shared with external suppliers, however the AEC recognizes that it will still be held accountable for such risks.'

In El Salvador, 'in the Supreme Electoral Tribunal (TSE), each Director or Head of each Organizational Unit is responsible for managing the electoral risks defined by the same in their respective area, which is backed by the highest authorities'. In Nepal, 'Each Division and Section Head owns the risk associated with their Division/Section'. In Bangladesh, Georgia, Iraq and Moldova, senior managers are also involved in these processes. In Guatemala, senior EMB managers collaborate directly with other state agencies.

In some countries, senior managers take all the responsibility. In Kenya, 'risks are owned by the Commissioners, the CEO and Directors who are charged with the overall management of the Commission'. In Bosnia and Herzegovina and Nepal, risk management is also shared with external agencies. As stipulated in the rule book on financial management and control in Bosnia and Herzegovina's Central Election Commission, the heads of organizational units and all employees are expected to take responsibility for risk management. For Namibia, even though it also responded that ownership was shared with other state agencies, risk management is contextually different, as the police and the army are also regularly involved. The EMBs of Guinea and Libya delegate responsibilities to other state agencies to address risks that are not managed internally.

### Box 9. Risk management responsibilities within the IEBC Kenya

The IEBC has developed a risk management structure with clear roles and responsibilities in the risk management process. The responsibilities of managing risks are assigned to committees and individuals.

The main role of the Board (the Commissioners) is to provide oversight of the implementation of the risk management framework, to set the tone and to determine the IEBC risk appetite. Below the Board is the Audit and Risk Committee, whose role is to help ensure that the IEBC maintains an effective risk management process.

The IEBC also has various committees charged with fulfilling its mandates. The committees are expected to undertake their risk management oversight role by understanding the risks that may affect the directorates that they provide oversight of and by obtaining feedback from management on how these risks are being managed.

### Box 9. Risk management responsibilities within the IEBC Kenya (cont.)

The IEBC Secretary/CEO is the head of the Secretariat. He or she ensures that risk management processes are implemented in all directorates and counties and is responsible for the implementation of the IEBC's risk management policy. The Risk Management Committee comprises directors and is chaired by the CEO. The Committee is charged with implementation and operationalization of a sound system of risk management and internal controls. It supports the Commission's Secretary in identifying and managing strategic risks on a quarterly basis, among other things.

The County Risk Management Committees were created in response to a review of the risk management policy. These committees comprise the Constituency Election Coordinators and are chaired by the County Election Managers. There are 47 such committees in the country. They perform the same role as the Risk Management Committee but at the county level.

The Commission has appointed risk champions at the directorate and county levels. Their main responsibility is to coordinate risk assessment and reporting at the directorate and county levels. The risk champions are the key drivers of risk management in the Commission. They are the custodians of the directorate and county risk registers.

All IEBC staff have personal risk responsibilities, which include communicating information known to them in the course of their work that is useful in identifying and evaluating threats and opportunities, effectively carrying out risk management measures in their area of responsibility and providing feedback on the effectiveness of the risk management processes and how to improve them.

The Commission also enters into inter-agency collaboration with other state agencies to manage risks arising from insecurity, to vet candidates for election and to resolve disputes involving political parties and candidates. The IEBC is also a member of the conflict analysis group under the Uwiano Platform for Peace, which is coordinated by the directorate for peacebuilding under the Office of the President.

## Embedding risk management

The objective of risk management is to improve organizational performance. The successful embedding of risk management is demonstrated by the consistency of risk considerations at all stages of organizational activities and by responsible staff, regardless of their rank or seniority. This level of embedding can only be achieved by a deliberate effort to align the risk management process with corporate objectives. Many organizations are guided by the generic principles offered by the ISO 31000 (2018: 3–4)—that is, risk management should be integrated into business operations, structured and comprehensive, customized, inclusive, dynamic, based on best available information, sensitive to human and cultural factors, and continually improved.

For EMBs wishing to apply these principles, an initial step may be to contextualize them to their organizations' business frameworks. In practical terms, this implies considering *how* to incorporate risk management into an EMB's organizational processes and *who* will be responsible for doing so.

### Approaches and opportunities

International IDEA (Alihodžić 2016: 22–24) outlines two approaches in which EMBs embed risk management. The first is an incremental approach, whereby an EMB progresses slowly. This (step-by-step) approach is less complicated, as it starts with the utilization of existing resources and expands at a pace that fits a particular EMB.

The second option is a comprehensive approach (all at once), which is appropriate when broader institutional reform is on the agenda and resources are available. Although more complicated, the latter approach will achieve results much faster and with greater certainty if managed effectively. Regardless of whether an EMB is taking an incremental or a comprehensive approach to embedding risk management, it is recommended that it always start by taking stock of existing organizational resources that can be utilized for this purpose. Further, an EMB should ensure that the processes and structures created are sustainable.

#### Box 10. Findings of the 2019–2020 EMB survey on risk management in elections

**EMBs were asked about key internal challenges for implementing risk management.**

| Options included (multiple selections possible) | Number of responses |
|---|---|
| Lack of subject experts | 25 |
| Organizational culture | 21 |
| Insufficient infrastructure/equipment | 19 |
| Limited funding allocations for risk management | 18 |
| Lack of human resources | 15 |
| Other | 7 |

A major challenge for EMBs is a lack of internal subject matter experts on risk. For example, Croatia, Nigeria and South Africa specify a lack of subject experts to deal with risks related to IT. For Botswana, the challenge is integrating and actually using the ERM Tool and the related software.

### Box 10. Findings of the 2019–2020 EMB survey on risk management in elections (cont.)

Organizational culture seems to be another challenge mentioned by a large number of respondents. For New Zealand, this is the main internal challenge. Canada highlights the limited internal ability to identify and evaluate the scope of incidents in a timely manner and to address occurrences of non-compliance. Some challenges are related to financial limitations. Bosnia and Herzegovina's EMB deals with insufficient infrastructure and equipment due to the limited funding available. The lack of human resources is another important factor. In many instances, all responsibility for risk management is assigned to staff who have other responsibilities, which becomes a burden.

The Commonwealth Guide (Australian Government 2016a) suggests pursuing quick wins by linking risk management with governance processes, corporate planning, projects and programmes, audit and assurance, and resilience-building. In the context of an EMB's mandate, practical steps may be as follows:

- An EMB's leadership should integrate risk management into their strategy, establish risk appetite through the risk management policy, define risk management roles and responsibilities and review how risks are managed within the EMB.
- Risk management could become an integral part of an EMB's planning framework. Its strategic objectives can be the starting point for any risk identification process.
- An EMB's project and programme implementation might involve continually identifying and managing risk within and between projects.
- A clear understanding of an EMB's risk profile would enable the prioritization of its audit and assurance activities. The outcome of internal and external audit activities may influence the design of an EMB control framework.
- Increasing organizational resilience could help an EMB resist shocks and stresses and improve its ability to restore normal operations during and after crisis periods.

In this respect, the Commonwealth Guide (Australian Government 2016a: 15) further emphasizes that organizations may have specialist programmes and processes, including business continuity and disaster recovery, fraud control, workplace health and safety, and protective security.

It further explains: 'While a specialist program may lead to an increased focus and management of these risks, specialist programs may benefit from being connected to the entity's overarching risk management framework to ensure consistency. This can be achieved by adopting common terminology and processes across all programs.'

## Box 11. AEC's corporate plan

The AEC publishes its corporate plan annually, which sets out the organization's strategic direction for the coming years. For 2020–2021, the AEC outlined the following four key agency priorities:

1. Maintain the integrity of electoral and regulatory processes.
2. Prepare for and deliver electoral events.
3. Engage with our stakeholders through education and public awareness activities.
4. Maintain a capable and agile organization and continue to professionalize our workforce.

Along with these objectives, the AEC's corporate plan has five strategic risks that must be managed in order to achieve those objectives:

1. The Commonwealth Electoral Act and the AEC's current operating model loses relevance to the modern-day service delivery experience and expectation of electors and stakeholders, especially in the Covid-19 pandemic environment.
2. The AEC is unable to uphold electoral integrity and transparency against a changing environment of domestic and global threats.
3. The AEC fails to build trusting relationships with electors, political stakeholders and the government.
4. The AEC cannot source and maintain a capable and trained Australian Public Service (APS) and temporary election workforce.
5. The AEC is not properly positioned for the future and is unable to deliver its core business and services, as its systems and processes are not sustainable, relevant or modern.

The ownership of these risks has been identified at the senior management level. The AEC's governance committees have also established their terms of reference to exercise oversight of targeted strategic risks. On a regular basis, risk analysis and reporting have been presented by subject business areas to the governance committees for discussion, especially where risk is above tolerance levels. For example, the AEC has a low risk tolerance for causing employees physical harm while operating in a counting centre temporarily set up during an election. When assessing the suitability of such premises, additional spending for modifications and improvement of premises is approved by AEC officials in order to meet the minimum standards for working conditions. This demonstrates that, where total funding for an election is limited, resources can be prioritized to mitigate risk where tolerance is low in a relatively speedy manner.

### Box 12. IEBC Kenya: strategic plan 2020–2024

Kenya's IEBC has developed a strategic plan within the context of its constitutional mandate and the Kenya Vision 2030 (a long-term development blueprint for the country). The plan sets strategic goals and objectives to be realized over the five-year period from 2020 to 2024. It also takes into consideration the dynamic nature of the electoral environment as well as the expectations of Kenyans for the impending electoral boundary review, referendums and the 2022 general election.

The strategic plan focuses on six key result areas:

(i). strengthening corporate governance;
(ii). strengthening the legal framework;
(iii). effective conduct of elections (political parties and candidate management, dispute resolution, campaign management, election operations, results management, voter registration and maintenance of the register of voters);
(iv). public outreach (effective voter education, strategic partnerships, collaboration and communication);
(v). equitable representation (accessibility, boundary delimitation); and
(vi). strengthening strategic operations (strengthening the institutional capacities of the IEBC; managing risk within the IEBC; strengthening information and communication technologies in elections and operations; strengthening the finance function and capacity for improved service delivery; strengthening the IEBC's procurement, warehousing and logistics functions; and strengthening the IEBC's planning, research and development functions).

In order to achieve the above objectives, the IEBC has embedded a risk matrix into the strategic plan that points to risks that are identified and require mitigation to enable the realization of the above focus areas. Risks have been assigned to the relevant risk owners. For more details, see the IEBC risk matrix in Annex G.

## Engaging and collaborating on risk

Once formal risk management elements are embedded in an EMB structure—linked to objectives, work processes and staff roles—the communication and consultation processes within an organization will put the risk management system into motion. Effective communication requires consultations between relevant stakeholders and the transparent, complete and timely flow of information between decision-makers.

## How to communicate risk

Frigo and Anderson (2011: 6) argue that each organization that starts with risk management needs to develop related communication processes, target audiences and reporting formats. However, they also emphasize the need to keep things simple, clear and concise while clearly reflecting the relative importance or significance of each risk.

Communication of risk within an EMB also involves sharing the outcome of the communication process with internal and external stakeholders. The EMB's management and board should ensure that identified risks are communicated through the escalation process (taking issues up the management chain) to ensure that risks are addressed appropriately. Risk communication must be supported by risk management tools which include risk registers, management risk reports, risk heat maps and a risk matrix (for practical insights and examples of AEC, Elections Canada and IEBC practices, see Annexes D, F and G). Many EMBs have already had substantive experiences with risk reporting and communication through the use of some kind of register that records risks, which—according to the ERM survey (see the survey findings in Chapter 1)—is the most common risk management document developed by EMBs. Also, the existence of a risk communication procedure is somewhat common.

### Box 13. IEBC Kenya risk reporting

To prevent and mitigate risk, the IEBC aims to ensure that knowledge about risk is effectively shared across the organization and with external stakeholders. The reporting of risks ensures that:

1. There is appropriate sharing of risk intelligence across the IEBC that can result in better appreciation of risks and refinement in terms of how identified risks are managed.
2. The Commission Secretary obtains the relevant information on risks required to help ensure that risks are properly managed and reported.
3. Everyone understands what the risk framework is, what the risk priorities are and how their particular responsibilities fit into that framework.
4. Lessons are learned and communicated to those who can benefit from them.
5. Each level of management receives regular assurance about the management of risk within their area of control.

Management and the Commissioners ensure that identified risks are communicated through the escalation process to ensure that risks are addressed appropriately. Risk communication is supported by risk management tools, which include risk registers, management risk reports, heat maps and a risk matrix (see Annex G).

The Commonwealth Guide (Australian Government 2016a) emphasizes the importance of communication and consultation with external stakeholders, such as other state agencies, suppliers and the wider community. This may be particularly important for addressing external risks. The Covid-19 pandemic is an example where EMBs must consult about risks with local and national health authorities while planning an electoral event.

### Box 14. Findings of the 2019–2020 EMB survey on risk management in elections

**EMBs were asked how information on risks was reported within their organizations.**

| Options included (multiple selections possible) | Number of responses |
|---|---|
| Through regular internal reporting processes | 31 |
| Through reporting processes designed specifically to convey information on electoral risk | 17 |
| Through exchanges with external (state and non-state) actors | 23 |
| Other | 2 |

Most EMBs report risks through regular internal reporting processes, while fewer EMBs have designated processes for conveying information on electoral risks. Over half of respondents indicated that there was an exchange on risks between an EMB and external stakeholders.

In Peru, the information is systematized in a risk matrix that contains assessed risks, which is then distributed to those involved in the electoral process. In Indonesia, information on risks is disclosed according to internal reporting schedules and sent to the government. A similar practice exists in Norway. Mongolia's EMB engages in an exchange of information about risks with NGO observers and international organizations through official communication methods.

In Kenya, the IEBC works with civil society and government agencies under the Uwiano Platform for Peace to address insecurity and communal conflicts. During elections, the EMB works with various stakeholders to establish a situation room where issues of gender-based electoral conflicts are discussed and common action undertaken.

### How to address shared risks

Shared risks may include risks across different functional units of an EMB and risks shared with other organizations. Failure to identify and manage shared risks effectively may, therefore, impact not only an EMB but also a broad range of stakeholders. Commonly shared risks within EMBs include risks which threaten the integrity of their service delivery. The impact of Covid-19 on communities during an election is a good example of shared risks between EMBs and a range of health authorities. Risks shared with other stakeholders may include risks related to safety and security, such as natural disasters, acts of terrorism, cyberattacks, public health risks and infrastructure failures.

EMBs should, therefore, work with stakeholders to better understand common threats and shared vulnerabilities and to optimize their collective ability to prevent, manage and recover from disruptive events. For this, EMBs need to educate their staff to identify and manage shared risks with other EMB departments, external agencies and service providers.

## Box 15. Managing shared risks

### AEC's delivery of Eden-Monaro by-election

In July 2020 the AEC delivered a by-election in the electorate of Eden-Monaro. A by-election is conducted when electors in a single federal electoral division vote to elect new members of the House of Representatives. This was the first electoral event the AEC was responsible for planning and delivering since the start of the Covid-19 pandemic.

At the time, a number of strict health orders were in effect in order to protect the health of election workers, voters and the general public.

The AEC consulted with Australia's chief medical officer to set up a centre to count paper ballots that operated in line with health protocols. The procedures were then communicated to staff through daily briefings to ensure consistent compliance.

Changes in voting procedures such as queue control and the use of hand sanitizer were communicated to voters through social media and the mainstream media.

The main advantage of using a risk lens when communicating with external audiences is a greater likelihood that those impacted by the risk will receive the information they require.

### Canada's Critical Election Incident Public Protocol

**The protocol:** Canada's Critical Election Incident Public Protocol was a mechanism used to communicate with Canadians during the 2019 general election in a clear, transparent and impartial manner if there was an incident that threatened the election's integrity (e.g. hacking of a government website or widespread disinformation).

The protocol is grounded in the view that any announcement during an election campaign that could have an impact on the election should best come from a trusted, non-partisan source, in this case senior public servants.

## Box 15. Managing shared risks (cont.)

**The panel:** The panel comprised senior public servants who had extensive experience in national security, foreign affairs, democratic governance and legal perspectives, including a clear view of the democratic rights enshrined in the Canadian Charter of Rights and Freedoms. The panel met regularly during the writ period and was kept apprised of the threat environment on an ongoing basis.

**The threshold:** The protocol is not used as a means to referee an election, and the threshold for making an announcement is very high and limited to exceptional circumstances. These considerations are assessed against various parameters, including the scope and impact of the incident(s). In respect of the type of incidents at issue, the protocol stipulates that the focus should be on interference that threatens the integrity of a general election.

**Announcements:** The panel must reach consensus on any decision to make an announcement. Barring any national security concerns, Canadians are informed of what is known about the incident and any steps they should take to protect themselves.

(For more information, see Democratic Institutions Secretariat, Privy Council Office, Government of Canada.)

### Public sensitization on how to vote amid Covid-19 in Kenya

In October 2020 the IEBC developed protocols for the conduct of electoral activities under the conditions of Covid-19. The by-elections held on 15 December 2020 were the first conducted since the pandemic began. The Commission liaised with the Ministry of Health in developing Covid-19 prevention and management protocols. The protocols were developed out of a realization that elections have the potential to result in the transmission of the virus to a large number of people during electoral activities including the registration of voters, the registration of candidates, campaigns, partner and stakeholder engagement, voter education, electoral training, voting and management of results.

The Commission responded by putting in place strategies to ensure system-wide compliance with Covid-19 prevention and management protocols, which helped fix the missing link between public health concerns and electoral management. The guidelines provided in these protocols (IEBC 2020) included the following:

- *Use of face masks.* All staff, stakeholders and the general public had to wear face masks at all times.
- *Use of alcohol-based sanitizers* by everyone participating in an electoral process.
- *Avoiding gatherings and crowds.* The Commission in collaboration with other authorities enforced the guidelines issued by the Ministry of Health at all social and political gatherings, including meetings and crowds.

## Box 15. Managing shared risks (cont.)

- *Implementation of social and physical distance.* Physical distancing (1.5 metres) had to be maintained in all places, including polling/registration centres, offices and stakeholder engagement meetings.
- *Cleaning, disinfection and ventilation of venues and surfaces.* Mechanisms were put in place to ensure frequent cleaning of all high-touch surfaces and objects (computers, the Kenya Integrated Election Management System [KIEMS]), and steps were taken to ensure that indoor office spaces/venues had adequate ventilation to increase air circulation.
- *Preventing physical contact and minimizing the sharing of general items.* The Commission encouraged people to bring and use their own items such as pens or writing materials.
- *Temperature checks.* Temperature checks were conducted with non-contact thermometers during voter registration, at polling stations, during other Commission events and at Commission offices to ensure that anyone with a high temperature (more than 37.5 degrees Celsius) was advised to seek medical attention.
- *Promoting healthy hygiene practices.* The Commission provided soap and water at all entry and exit points to promote high standards of hygiene.
- *Protecting vulnerable populations.* Persons with proven pre-existing medical conditions as well as elderly people, the disabled, lactating mothers, pregnant women and the sick were given priority. The protocols also provided specific guidelines and procedures that prescribed additional interventions while conducting electoral activities.

Finally, the protocols contain a section on risk management that identifies risks associated with the Covid-19 pandemic and their mitigation, as well as the impact of the implementation of the protocols.

## Box 16. Findings of the 2019–2020 EMB survey on risk management in elections

**EMBs were asked about key *external* challenges for implementing risk management.**

| Options included (multiple selections possible) | Number of responses |
|---|---|
| Budget allocations | 24 |
| Political environment | 20 |
| Government policies/legislation | 18 |
| Social environment | 13 |
| Community engagement | 10 |
| Other | 2 |

### Box 16. Findings of the 2019–2020 EMB survey on risk management in elections (cont.)

The survey finds that the most common external challenges for an EMB are insufficient budget allocations and funding dependency on the government. Costa Rica's EMB notes that its budgetary allocation does not allow it to earmark sufficient resources for risk prevention and mitigation of electoral risks. The same goes for Mexico, where the EMB highlights the fact that decisions on budget allocation and/or reductions do not allow risk management to be prioritized.

Government policies and legislation are considered to be another external challenge. Guinea's EMB highlights the fact that, since such policies and legislation are the exclusive domain of the National Assembly and the president of the republic, the EMB is unable to address systemic risks. In Nigeria, the socio-economic conditions create significant challenges for the risk management effort (risk levels and mitigation strategies). For example, related risks materialize through violent attacks, protests and vote-buying.

A significant number of countries also point to challenges with community engagement. Portugal's EMB encounters challenges when it comes to the public's understanding of the EMB's decisions, communication with the media and electoral stakeholders. In New Zealand, the challenge is in getting broader buy-in and ownership of risks relating to general elections that are owned by other agencies—that is, agencies other than the EMB. Another important challenge that El Salvador's EMB has considered is how to face and neutralize content that circulates on social media, mainly in electoral periods, which undermines institutional work.

## Reviewing and continuously improving risk management

Formalizing and implementing risk management within an EMB is not a one-off event. In an EMB environment, objectives and capabilities change over time, as do its risks, risk appetite and exposures. To ensure that new risks are identified and that existing risks remain appropriately managed, EMBs must continuously review their risk management framework. This requires mechanisms, both formal and informal, that provide assurance on the efficiency, effectiveness and relevance of the EMB's approach to risk management. The mechanism should also ensure that good risk management practices are recognized and rewarded.

According to the ISO 31000 (2018: 14), the ongoing monitoring and review process aims to 'assure and improve the quality and effectiveness of process design, implementation and outcomes' and should 'be a planned part of the risk management process, with responsibilities clearly defined'.

The Commonwealth Guide (Australian Government 2016a: 26–28) proposes that three aspects be considered in the assessment of the performance of an organization's risk management framework. These include value added (the extent to which risk management contributes to achieving the organization's objectives), maturity (if the risk management framework is fit for purpose and appropriate) and compliance (the extent to which it is consistently applied). Accordingly, the practical steps that EMBs should undertake include:

- a periodic review of the risk management framework in terms of its relevance for an organization (various sources suggest that this be an annual exercise);
- a review of compliance with, and the application of, the framework (this could be done through regular checking and monitoring, management review or an external review);
- a review of the risk profile (which may relate to a specific electoral cycle; see the example below); and
- a review of individual risks and the controls that are in place to manage them.

According to the ISO 31000 (2018: 14), 'the results of monitoring and review should be incorporated throughout the organization's performance management, measurement and reporting activities'.

### Box 17. Assessing and addressing risks from cyberattacks in Canada

In 2011 Canada experienced a robocall scandal in which thousands of voters in almost 250 ridings (constituencies) reported receiving automated phone messages falsely telling them that their polling stations had been changed. This operation aimed to suppress voter turnout. Elections Canada's investigations found that domestic political actors were responsible. The incident prompted Elections Canada to set up an Electoral Integrity Office to identify domestic and international cyberthreats, assess risks and set up systems to track and prevent cyberattacks by foreign actors, political operatives or individuals who might want to disrupt elections or manipulate the results (Van der Staak and Wolf 2019).

### Box 18. IEBC's approaches to identifying its risk profile

A risk profile can relate to a whole entity or a part of an entity or be otherwise defined. The following are techniques that the IEBC uses to determine risk profiles:

1. *Questionnaires and checklists.* Structured questionnaires and checklists are used to collect information to assist with the recognition of significant risks.
2. *Workshops and brainstorming.* Ideas are collected and shared, and events that could impact objectives, stakeholder expectations or key dependencies are discussed.
3. *Inspections and audits.* External and internal audits are used to identify risk exposure.

## Box 18. IEBC's approaches to identifying its risk profile (cont.)

4. *Stakeholder feedback.* Feedback is obtained from staff and third parties (including political parties, customers, suppliers and other development partners) on possible risk exposure. As a public body, the Commission considers its beneficiary to be the public and therefore would be keen to work on any information received from external stakeholders.
5. *SWOT and PESTLE analyses.* The SWOT (strengths, weaknesses, opportunities and threats) and PESTLE (political, economic, social, technological, legal and environmental) techniques offer structured approaches to identifying risks. They are used to analyse the operational environment and identify key obstacles in achieving the desired results. These steps should include an analysis of relationships and of the perception and values of suppliers, users and other key stakeholders.
6. *Benchmarking.* The Commission benchmarks its activities with similar organizations in the region as a way to identify risk within its operations.

## Box 19. Findings of the 2019–2020 EMB survey on risk management in elections

**EMBs were asked about how they identified risks to their electoral processes.**

| Options included (multiple selections possible) | Number of responses |
|---|---|
| Through the evaluation of past elections | 40 |
| Through internal planning processes | 33 |
| Through internal consultations focused on the identification of risks | 32 |
| Through consultation with external stakeholders focused on the identification of risks | 23 |
| Through feedback from election observation organizations | 24 |
| Other | 6 |

EMBs have multiple avenues available for identifying risks in electoral processes. The most common is through the evaluation of past elections. This entails the organization of post-election evaluation seminars, conferences, workshops and surveys. Findings are used to better identify risks for subsequent electoral cycles. However, this practice is intertwined with other methods for identifying risks.

Some countries (e.g. Canada, Finland, Slovenia, South Africa and Zanzibar) indicate that they utilize all of the options provided in the survey question. Internal planning processes and internal consultations are also broadly used to identify risks that EMBs face. In addition to the options offered, Bosnia and Herzegovina's EMB indicated that media monitoring is used to identify election-related risks.

### Box 19. Findings of the 2019–2020 EMB survey on risk management in elections (cont.)

Coordination with external stakeholders is also important. For New Zealand's EMB, consultations and coordination with external stakeholders are a new practice adopted with the support of independent experts. In a large number of countries, EMBs refer to election observation reports and recommendations to identify potential risks. Before every election in Azerbaijan, the election commission carries out an evaluation of past elections and considers election observers' feedback to identify risks.

# 4. Building a positive risk management culture and capability

## Risk management culture

A positive risk culture is one where staff at every level appropriately manage risk as an intrinsic part of their day-to-day work. Such a culture supports an open discussion about uncertainties and opportunities, encourages staff to express concerns and maintains processes to elevate concerns to appropriate levels (Australian Government 2016b).

The Commonwealth Guide (Australian Government 2016a: 15) finds that 'decisions are often made, and risks managed, without complete information, with inadequate resources and against competing priorities. In these circumstances, a strong risk culture will support the proper management of risk.' The Commonwealth Guide also states that 'Culture is more than just complying with your entity's risk management framework. The behaviours and attitudes to risk are just as important as the framework.' The ISO 31000 (2018: 9) states that 'human behaviour and culture significantly influence all aspects of risk management at each level and stage' and that 'the dynamic and variable nature of human behaviour and culture should be considered throughout the risk management process'.

### Box 20. Findings of the 2019–2020 EMB survey on risk management in elections

Twenty-one of the 43 EMBs that responded to the ERM survey specifically indicate that a lack of positive risk management culture is one of the key challenges for implementing risk management. New Zealand's EMB highlights its effort to make risk management part of its culture by making it an 'aspect of project management and reporting'.

For El Salvador's EMB, consolidation of the organizational culture related to risk management requires 'greater situational awareness, commitment, and participation at all levels'. The EMBs of Indonesia and Nigeria acknowledge that risk management must be a culture in organizations, and that it needs to be continuously strengthened.

## Box 21. IEBC Kenya risk management culture

According to IEBC (2017a), its risk culture reflects the degree to which the principles of risk management are embedded across an organization. Features of a mature risk culture include the following:

- Management and staff involved in risk management have a common understanding of the necessity of risk management and the benefits that arise from it.
- Management and staff have been trained on the principles of risk management and the application of standards.
- Management and staff consistently understand and embrace both formal and informal risk management processes and understand the relationship between these processes.
- Risk management competencies are included in job descriptions, and appraisals measure the degree to which risk management responsibilities have been met.
- Managers feel a sense of responsibility towards risks and mitigating controls related to their areas.
- Managers provide assurance on the effectiveness of their risk identification and ongoing management of risks.
- A culture of risk escalation exists.
- Risk management is part of the regular process for each department and is regularly discussed at meetings.
- The terminology used in relation to risk management is consistent.

When it comes to strengthening a risk management culture, 'leaders and senior managers can play a pivotal role, acting as role models to more junior staff by detecting and preventing risks and hazards themselves thereby promoting risk management issues in the organization' (Cormican 2014: 408). Also, 'ongoing communications from directors and senior management will serve to reinforce and nurture the risk management culture' (Frigo and Anderson 2011: 7).

Some EMBs may already have an organizational culture conducive to risk management. Namely, staff across the organization are risk-aware and feel free to share information about risks, while different departments and regional offices collaborate and communicate challenges to the EMB leadership. In such an organization, risk management will find a natural habitat. An EMB where decision-making is characterized as positional, authority-based and directive, is by nature not a conducive risk culture. To foster the development of a positive risk culture, an EMB's leadership should act as role models, provide affirmative messages about the importance and value of risk management processes and provide incentives. Quick gains from the risk management process that can be used as examples to demonstrate benefits for an organization will help. Key features that indicate a positive risk culture include trust between staff and senior managers, an absence of blaming and shaming of employees for honest mistakes and misjudgements, and authentic leadership demonstrated in times of uncertainties such as the ongoing pandemic.

## Risk management capability

An important factor in successful risk management practices is an organization's ability to implement its risk management framework. When it comes to ensuring that an EMB has the internal capability required to implement the risk management process effectively, senior management will yield good returns from investing in strengthened capability of its people and its risk systems and tools.

### People capability

The capability of an organization's people is strengthened through learning and development, access to information, peer support, induction, recognition and rewards, and performance management. Cormican (2014: 408) stresses that 'effective training is imperative to effective risk management' and that 'a program of continuing ERM education for directors and executives is needed'. Most EMBs already have a culture that strongly values professional development—through national and international training programmes—for permanent and temporary staff. However, only a few EMBs train their staff in risk management matters. Therefore, for most EMBs, the existing capacity-building foundations could be expanded to cover the topic of risk management in electoral processes.

### Box 22. Findings of the 2019–2020 EMB survey on risk management in elections

**EMBs were asked to indicate capacity-development practices implemented by their organizations.**

| Options included (multiple selections possible) | Number of responses |
|---|---|
| Capacity-building on risk management is provided to all staff in the organization | 9 |
| Capacity-building on risk management is provided to senior management | 15 |
| Capacity-building on risk management is provided to selected staff in HQ | 17 |
| Capacity-building on risk management is provided to selected staff in subnational offices | 9 |
| Capacity-building on electoral risk management is provided to external stakeholders | 7 |
| Other | 4 |

### Box 22. Findings of the 2019–2020 EMB survey on risk management in elections (cont.)

EMBs offer limited capacity-building on risk management issues in their organizations. Slightly more than one-third of EMB respondents offer such opportunities only to selected staff at their headquarters and to field and senior management. Significantly fewer offer such opportunities to all staff in the organization and to the staff in subnational offices.

Malawi's EMB confirms the importance of specialized knowledge for the management of electoral risks. Botswana's EMB points to the benefits of a training programme on risk management implemented by International IDEA and peer exchange with other EMBs on the topic. Peru's EMB refers to the lack of specialized staff with risk management knowledge. Maldives' EMB conducts an internal symposium to address the obstacles and risks faced throughout an election. In this symposium, a paper is presented by each section, division and unit concerning risks and obstacles and offers solutions to prevent and mitigate them.

When developing and implementing training on risk management, EMBs should consider several elements that reflect the division of risk management responsibilities within an organization. For example, risk management training for an EMB's senior management should be integral to their leadership development and give them a full overview of the process within an organization. It should also reiterate the purpose and potential benefits of the process for making informed executive decisions and explain how to foster a risk management culture. Training for programmatic and project managers should focus on the identification and assessment of risk and controls. All other EMB staff should undergo general management training that builds their capability to identify, measure, record and report risks, as well as an understanding of internal procedures to do so.

Since risk management is an evolving process, refreshment training should be offered periodically to all staff. Investing effort to identify and build the capacity of risk champions may contribute to the efficiency of training and help sustain these capabilities between training sessions. Also, the use of positive examples from an organization will help to reinforce a shared understanding of the process and standards of good risk management.

### Box 23. Risk management training

**The AEC's approach**

The AEC's risk management policy states that all staff are expected to actively participate in the management of risk, including identifying risks, contributing to risk assessments and monitoring risk plans within their area of responsibility.

## Box 23. Risk management training (cont.)

In 2020 the AEC's Risk Unit launched a series of new training initiatives to ensure that staff have the capability and knowledge to perform their roles and meet their obligations. The training approach was combined with the launch of the AEC's Risk Management System (ARMS), an enterprise risk management system.

To maximize the value of ARMS, the training approach developed involved sessions delivered across the AEC's network, which provided an overview of the AEC's risk management framework and focused on how to identify and describe risks, and how to use ARMS to undertake risk assessments.

The training was initially delivered in person; however, with the outbreak of the Covid-19 pandemic, it moved to online delivery. Later in the year, an e-learning module was developed for the AEC's learning management system which covered similar content and is now included in the AEC's national induction programme for new staff. In 2021 a separate risk management training approach was designed and delivered for operational leaders, which involved a video, a case study and team discussions.

The training options provided are based on delivery to all levels of staff. In addition, the Commonwealth Government agency Comcover also offers a targeted set of training and awareness activities for Commonwealth senior executive staff which focuses on a strategic approach to risk management, including fostering a positive risk culture and providing risk leadership.

### IEBC training

The IEBC's risk management framework emphasizes the need for regular training for the Commissioners, Audit and Risk Committee members and staff to enable them to understand and execute their risk management responsibilities. In the past, the IEBC has conducted training for Commissioners, members of the Audit and Risk Committee, Directors and risk champions. For example, the IEBC organized an enterprise-wide electoral risk management training event in July 2019. The overall objective was to strengthen the IEBC's capacity in implementing its enterprise-wide risk management framework. Specifically, the workshop aimed to accomplish the following:

- raising awareness and enhancing understanding of the objectives, principles and main components of the IEBC's risk management strategy;
- familiarizing risk champions with the IEBC's new risk management reference documents and building their capacity to utilize them; and
- equipping risk champions with the knowledge and tools required to replicate the training for other IEBC county and directorate officials across the country.

During the training, participants were guided through all aspects of the policy, the process and the risk management tools that they will work with. The training included practical exercises whereby participants completed risk registers, which they will be required to complete on a quarterly basis. At the end of the workshop, participants understood their roles and responsibilities as

### Box 23. Risk management training (cont.)

risk champions and had acquired the requisite skills to support the work of the Audit, Risk and Compliance Directorate in coordinating the IEBC's risk management framework.

Plans are in place to train the remaining staff in the near future. The staff in charge of coordination of risk management at the Audit, Risk and Compliance Directorate continuously undergo professional training.

## Risk systems capability

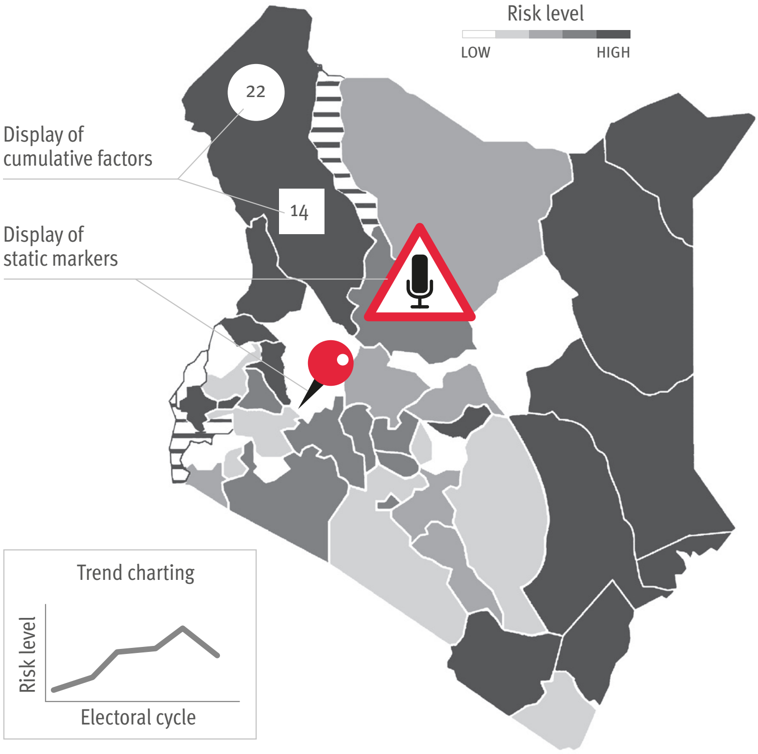
Risk systems and tools deliver the capability to store, integrate and analyse risk data, disseminate and share risk information and automatize risk process workflows. Some of the functions provided by risk systems and tools include:

- storage of risk information (a centralized register of identified risks and related decisions made by an organization);
- monitoring of key risk indicators (space where observable indicators and values are specified and tracked over time);
- analysis of risk information (analytical outputs in the form of narrative descriptions, charts and maps);
- sharing of risk information (risk status reports and risk and compliance dashboards); and
- automation of risk process workflows (risk tasks, data or files are routed between people based on predefined rules).

Risk systems and tools will be most effective when they are appropriate to an EMB's needs, well maintained and complemented by training and workplace support. Due to the dynamics of electoral risks throughout an electoral cycle, an EMB will potentially face a large influx of data that is of relevance for assessing and analysing risks. This data may come from different sources (different departments, regional offices, external organizations), be in different formats (qualitative, quantitative, photo, video, etc.) and be received by different EMB units.

Analysis of risk data and responses may be carried out at the level of functional teams and departments and at the level of an organization. In the latter case, to obtain a holistic understanding of risk dynamics in order to effectively focus prevention and mitigation efforts on specific risks and regions affected, an EMB might benefit from the technical capability to integrate all risk data into a single database. Sophisticated software tools will provide such capability. Further, they may provide for data analysis through the creation of visuals, such as trend charts and geographical maps that are easy to share, while the content is easy to comprehend. Ultimately, it will serve the purpose of making timely and well-informed decisions.

## Figure 3. Visualization of risks



*Source:* Alihodžić, S., 'Electoral violence early warning and infrastructures for peace', *Journal of Peacebuilding & Development*, 7/3 (2012), pp. 54–69, <https://doi.org/10.1080/15423166.2013.767592>.

### Box 24. Findings of the 2019–2020 EMB survey on risk management in elections

The survey finds that Botswana's EMB compiles a risk matrix and risk register generated through MS Office applications. In Peru, EMB risk information is communicated through the information security management system used for document processing, verification and control. Latvia's EMB has an IT system for risk management. The EMBs of Bosnia and Herzegovina, Kenya, Namibia, Nepal and Nigeria use the ERM Tool developed by International IDEA.

The ERM Tool is the only instrument freely available to EMBs for the purpose of strengthening their capability to manage electoral risks. The tool takes the form of a desktop software application that integrates three modules.

### Box 24. Findings of the 2019–2020 EMB survey on risk management in elections (cont.)

The first module consists of a customizable digital library that is prefilled with 36 electoral risk factors covering both the electoral process and the context in which elections take place.

The second module utilizes GIS (geographic information system) technology and digital databases (database server) to enable users to create country- and election-specific analytical models that comprise selected risk factors, to upload and analyse data in different formats (e.g. generate geographical maps or trend charts) and to create and maintain a digital risk and action register.

The third module is a digital library with approximately 100 action points based on good practices worldwide.

Because risk management in elections is still maturing, there is significant scope for further development and refinement. Along these lines, International IDEA has shared the ERM Tool's source codes (Alihodžić 2020) openly so that interested organizations can further advance the software or customize it for their specific needs.

As reiterated in several sections of this Guide, the adoption and implementation of the risk management concept is often an incremental process, even when an initial effort is comprehensive. The incremental nature generates the need to periodically assess and evaluate the progress made by an EMB. Risk management experts and scholars already offer numerous assessment tools, commonly referred to as risk management maturity assessment frameworks, which can be applied in a straightforward manner or customized for electoral processes. One such tool, the Risk Management Capability Maturity Scale, is customized for use by EMBs (see Annex C).

# 5. List of resource materials

Risk management is often described as both an art and a science. It is an art in a sense that it requires vision, inventiveness and creativity. It is a science in that it requires methodological rigour and objectivity based on evidence. Both the art and science of risk management are cultivated through practice. The literature on risk management is extensive and often focused on the expert audience. Therefore, it is very common that specific risk management policies are followed by a range of support resources developed to provide practical guidelines, examples and tips for implementation. Examples of how the AEC tailors the Commonwealth Risk Management Policy have been referenced across this Guide.

Similarly, this Guide offers seven annexes with practical information to help EMBs navigate through critical terms and concepts: these include practical templates and tools adopted and developed by the Australian Electoral Commission, Elections Canada and the Independent Electoral and Boundaries Commission of Kenya.

Annex A. Glossary of terms

Annex B. Risk management process

Annex C. Risk Management Capability Maturity Scale

Annex D. Australian Electoral Commission: risk matrix and escalation table

Annex E. Key risks faced by electoral management bodies

Annex F. Elections Canada: risk assessment criteria and risk register

Annex G. IEBC Kenya: risk matrix, risk register template and heat map

# References

Alihodžić, S., 'Electoral violence early warning and infrastructures for peace', *Journal of Peacebuilding & Development*, 7/3 (2012), pp. 54–69, <https://doi.org/10.1080/15423166.2013.767592>

—, *Risk Management in Elections*, Policy Paper No. 14 (Stockholm: International IDEA, 2016), <https://www.idea.int/publications/catalogue/risk-management-elections>, accessed 7 May 2021

—, 'Electoral Risk Management Tool source codes are now available to democracy practitioners', International IDEA, 28 September 2020, <https://www.idea.int/news-media/news/electoral-risk-management-tool-source-codes-are-now-available-democracy>, accessed 4 May 2021

Australian Government, Department of Finance, 'Commonwealth Risk Management Policy', 1 July 2014, <https://www.finance.gov.au/sites/default/files/2019-11/commonwealth-risk-management-policy_0.pdf>, accessed 22 April 2021

—, Department of Finance, 'Implementing the Commonwealth Risk Management Policy—Guidance', 2016a, <https://www.finance.gov.au/sites/default/files/2019-11/implementing-the-rm-policy.pdf>, accessed 22 April 2021

—, Department of Finance, 'Comcover Information Sheet: Developing a Positive Risk Culture', 2016b, <https://www.finance.gov.au/sites/default/files/2019-11/Risk-Culture.pdf>, accessed 26 April 2021

Cormican, K., 'Integrated enterprise risk management: from process to best practice', *Modern Economy*, 5/4 (2014), pp. 401–13, <https://doi.org/10.4236/me.2014.54039>

Frigo, M. L. and Anderson, R. J., *Embracing Enterprise Risk Management: Practical Approaches for Getting Started* (Durham, NC: Committee of Sponsoring Organizations of the Treadway Commission, 2011), <https://www.coso.org/Documents/Embracing-ERM-Getting-Started.pdf>, accessed 22 April 2021

Independent Electoral and Boundary Commission (IEBC), 'Risk Maturity Assessment Report', March 2017a, unpublished

—, 'Risk Management Framework', 2017b, unpublished

—, 'Protocols for Conducting Electoral Activities in the COVID-19 Context: Quest for Responsive Credible Elections in a Global Pandemic', 2020, <https://www.iebc.or.ke/uploads/resources/OFt91j0dYQ.pdf>, accessed 26 April 2021

International IDEA, Electoral Risk Management Tool (ERM Tool), 2013, <https://www.idea.int/data-tools/tools/electoral-risk-management-tool>, accessed 4 May 2021

International Organization for Standardization (ISO), *Risk Management—Principles and Guidelines*, ISO 31000: 2009, <https://www.iso.org/standard/43170.html#:~:text=Risk management – Principles and guidelines,-This standard has&text=ISO 31000:2009 provides principles,to any industry or sector>, accessed 7 May 2021

—, *Risk Management—Guidelines*, ISO 31000: 2018, <https://www.iso.org/standard/65694.html>, accessed 7 May 2021

Kenya Vision 2030, Official website, <https://vision2030.go.ke/>, accessed 7 May 2021

Van der Staak, S. and Wolf, P., *Cybersecurity in Elections: Models of Interagency Collaboration* (Stockholm: International IDEA, 2019), <https://doi.org/10.31752/idea.2019.23>

# Annex A. Glossary of terms

The list below includes common terms and definitions used in risk management–related communications and literature.

| Term | Definition |
|---|---|
| Control | A measure to modify risk. Controls are the result of risk treatment. Controls include any policy, process, device, practice or other actions designed to modify risk. |
| Control owner | A person or entity with accountability for ensuring that the control activity is in place and is operating effectively. The control owner does not necessarily perform the control activity; however, if not conducting the control, they should maintain a level of oversight of its performance. |
| Risk | The effect of uncertainty on objectives. An effect is a positive or negative deviation from the expected. Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances or knowledge) and the associated likelihood of occurrence. |
| Risk analysis | A process aimed at comprehending the nature of risk and determining the level of risk.<br>Risk analysis provides the basis for risk evaluation and decisions about risk treatment. |
| Risk assessment | The process of risk identification, risk analysis and risk evaluation. |
| Risk appetite | A process aimed at comprehending the nature of risk and determining the level of risk. |

| Term | Definition |
|---|---|
| Risk evaluation | The process of comparing the level of risk against risk criteria. Risk evaluation assists in decisions about risk treatment. |
| Risk event | A risk event occurs when the conditions for the existence of the risk come together with a triggering action which leads to the creation of an event (can be either a positive or a negative event). Risk events lead to measurable effects which may lead to other effects and eventually lead to an undesirable consequence. |
| Risk identification | The process of finding, recognizing and describing risks.<br>Risk identification involves the identification of risk sources, risk events, their causes and their potential consequences. |
| Risk management | Coordinated activities to direct and control an organization with regard to risk. |
| Risk management framework | A set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout an organization. |
| Risk management process | The systematic application of management policies, procedures and practices to the tasks of communicating, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk. |
| Risk oversight | The supervision of the risk management framework and risk management process. |
| Risk owner | A person with the accountability and authority to manage a risk and any associated risk treatments—sometimes referred to as a risk steward. |
| Risk profile | A description of any set of risks. The set of risks can contain those that relate to the whole organization or part of the organization, or they may be defined in some other way. |
| Risk reporting | A form of communication intended to address particular internal or external stakeholders to provide information regarding the current state of risk and its management. |

| Term | Definition |
|---|---|
| Risk tolerance | The levels of risk-taking that are acceptable in order to achieve a specific objective or manage a category of risk. Risk tolerance defines the limits (quantifiable where practicable) that support the entity’s risk appetite. |
| Risk treatment owner | The person responsible for monitoring and reporting on progress in the implementation of the treatment plan. |
| Shared risk | A risk with no single owner, where more than one entity is exposed to or can significantly influence a risk. |
| Treatment | A treatment is a proposed control that has not yet been implemented. The term can also be used to refer to the process of selection and implementation of measures to modify risk. |

# Annex B. Risk management process

There are different methodologies that EMBs can adopt to manage risks. For this Guide, examples are based largely on ISO 31000:2018 *Risk Management—Guidelines*. What is vital, however, is that the process adopted provide a tailored, structured approach to understanding, communicating and managing risk in practice.

## Steps in the risk management process

The following steps are based on those used by the AEC, as outlined in its internal 'AEC Risk Management Guidelines' document, which shows AEC staff how to conduct risk assessments and risk treatments.

### Step 1. Establish the scope, context and criteria

This step includes defining the scope of the process/activity and understanding the external and internal context, while considering the objectives to be achieved.

A useful checklist for considering the external context is a PESTLE analysis, namely: Political and government; Economic/financial; Social and cultural; Technological; Legal and regulatory; and Environmental.

Internal factors that may influence risk exposure can include, but are not limited to, people, information, budget, technology and equipment.

*Tip:* External risks generally arise from conditions that one mostly cannot influence. Internal risks generally arise from decision-making within an organization and its use of internal and external resources.

### Step 2. Risk identification

The purpose of risk identification is to identify and describe risks that may help or prevent an organization in achieving its objectives.

It is important to remember that risks are managed within the context of the relevant objectives that the risk assessment relates to (e.g. at the strategic, enterprise, operational and project level). As a result, it is best to start with a clear understanding of the objectives and then consider the threats and opportunities that will influence the achievement of those objectives.

Risks should be described as events or incidents, not as failures of controls or processes. A process failure is the *cause* of a risk. Describing causes as risks will result in too many risks to be managed properly. Identifying risks as events provides a tighter focus.

One way to check whether a risk has been defined well is to ask whether, if the risk were to occur, the event in question could be visualized and a post-event analysis could be undertaken. If such an analysis cannot be conducted, it is probably not a risk.

Examples of how the AEC describes risks are as follows:

| Causes | Risk event | Consequences |
|---|---|---|
| Lack of supervision/training<br>Lack of monitoring and identification mechanisms<br>Lack of staff awareness<br>Lack of appropriate security controls<br>Accidental or deliberate release of information by a trusted insider<br>Hacking and cyberattacks | Release of confidential information | Privacy breach (including silent electors)<br>Breach of government security requirements<br>Financial impact<br>Adverse audit findings<br>Reputational damage |

Another way to describe a risk is in terms of the failure to meet an objective: this works well for governance- and compliance-type risks where a tangible event or incident may not apply.

| Causes | Risk event | Consequences |
|---|---|---|
| Ineffective design, development or delivery of governance framework<br>Poor understanding of learning needs and objectives<br>Late changes in procedures, policies and/or legislation<br>Ineffective evaluation | Failure of governance framework to facilitate improvements to good practice | Diminished compliance, professionalism and capability<br>Impact on business processes and time frames<br>Legislative, regulatory or policy breach<br>Inconsistent approach to implementation of policies and procedures |

*Tip:* One way to determine whether to have one or two risk events is whether the nature and level of the consequences are different. During a federal election, for example, the reputational impact of a member of the public being injured may differ from that of an election staff member being injured. In addition, the controls used to manage these risks may also be different.

### Step 3. Risk analysis

The risk analysis process seeks to establish the likelihood or probability of a risk occurring and the consequences or degree of impact on the EMB if it does occur. The likelihood and the consequence of a risk combine to establish the overall level of risk.

A risk matrix is a table that describes a range of possible likelihoods and consequences. This can be tailored to the nature of the EMB.

When determining the risk level, it is important to consider the impact of controls—for example, policies, processes and systems already in place to reduce the likelihood or consequences of a risk occurring. Controls should be rated in terms of their effectiveness in either preventing or reducing the impact of risks.

The assessment of a risk occurring (likelihood) or the impact of an event (consequence) can be subject to personal bias. For this reason, every step in the assessment requires communication and consultation. A good practice is that the assessment of risks be undertaken collaboratively in a workshop involving key stakeholders including external service suppliers where applicable.

### Step 4. Risk evaluation

The purpose of risk evaluation is to support decisions. Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required.

Once a risk has been identified and assessed, it must be evaluated to determine what further action is required. This decision is aided by an understanding of the EMB's risk appetite. Risk appetite is the amount of risk an organization is willing to accept or retain in the pursuit of its objectives. This can be further broken down into risk tolerance, whereby a more specific approach to taking risk for a particular category or type of risk (e.g. public or staff safety) can be articulated.

Actions may include accepting the risk, monitoring and maintaining existing controls, or further treating the risk, with monitoring performed by the relevant governing committees.

### Step 5. Risk treatment

This step involves developing further measures to reduce the level of risk to the organization if warranted based on an evaluation. A number of options are available to treat risks, including avoiding the risk, reducing its likelihood or impact, or sharing the risk with a third party.

It is important to note the difference between controls and treatments: controls are existing processes, whereas risk treatments are new or modified processes currently under development. A treatment only becomes a control after it has been fully implemented and deemed effective in modifying risk to an acceptable level.

### *Recording, monitoring and review, and reporting*

A risk register is a management tool that enables an organization or governing committee to understand its comprehensive risk profile. Its purpose is to inform the decision-making process, assist in the regular review of business (which in turn provides assurance on controls) and provide an opportunity for senior executives to review the agency's level of risk appetite and assess the effectiveness of risk treatments.

Monitoring and reviewing risks will highlight environmental, strategic and other factors that vary over time and that could change or invalidate the risk assessment and therefore impact the level of treatment required, its interdependencies with other functions and activities, and its relevance in the decision-making process.

Risk assessments should be updated as circumstances change, such as during a review cycle.

# Annex C. Risk Management Capability Maturity Scale

It is important that entities develop risk management frameworks and systems that are tailored to the needs of their organization. The risk management maturity assessment of an EMB will ensure that the risk management framework is fit for purpose by reflecting its size, complexity and risk culture. An example of a practical assessment scale is provided below, which is loosely based on maturity scales for risk management practice derived from the Comcover risk management benchmarking survey, which is administered by the Australian Government agency Comcover.

## Attributes of the Risk Management Capability Maturity Scale

Maturity levels are cumulative: completion of the maturity assessment will primarily involve gathering information about an EMB's current risk management practices. Methods used to gather information might include conducting interviews with management and staff, gathering and reviewing documents, carrying out site visits (where applicable) and conducting workshops and/or surveys.

| Initial | Developing | Defined | Integrated |
|---|---|---|---|
| There is no risk management policy or framework.<br>Risks are not recorded consistently.<br>There is no clear connection between risk assessments and decision-making. | Risk management policy and procedures in place but not integrated into operations or governance forums.<br>Inconsistent understanding of risk appetite/ tolerance. | Risk management framework is integrated into operations and governance forums.<br>Risk appetite/ tolerance for categories of risk is formally documented. | Risk management policy and risk appetite/tolerance statements are used to inform decision-making, and decisions are explained as such.<br>Governance framework |

| Initial | Developing | Defined | Integrated |
|---|---|---|---|
| Staff have little to no awareness of risk management practices and procedures. | No dedicated resources to manage the risk framework.<br>The reporting and consideration of risk issues is performed in an uncoordinated manner.<br>Work unit risks are reviewed annually; however, risks do not inform EMB business planning, budgeting and reporting processes. | There are dedicated resources to manage the risk framework and report on risks, and information is in turn shared with other areas such as audit and business continuity.<br>Enterprise-wide risks are considered in business planning, budgeting and reporting processes; however, there is no evidence of the identification of specialist categories of risk, such as fraud or business continuity in these processes. | actively assists with recording, monitoring and reporting on risks.<br>Responsibility for managing risks is clearly defined within the governance framework.<br>Risk information and data are stored in a central database which is accessible to staff.<br>The processes of identifying, assessing, monitoring, communicating and reporting risk are consistent across the entity.<br>The risk team is responsible for helping work units to consistently identify and evaluate risks.<br>The process of managing risk occurs at the policy, programme and/ or service delivery level and is evident in the collation and analysis of management information. |

Risk management is a continual process, and the proposed maturity indicators of the 'Integrated' level do not represent the end of this process. In recognition of this, a further level of organizational risk management maturity would include such features as:

- Real-time information is readily available and used to identify, analyse and assess risks and trends.
- The costs of risk management activities are managed within the operational budget.
- Risk resources are allocated based on information analysis.
- Key risk indicators are used to measure the overall performance of the risk framework.

# Annex D. Australian Electoral Commission: risk matrix and escalation table

The information in this annex is published with the kind permission of the Australian Electoral Commission. The risk matrix and escalation table are not publicly available.

## Risk Matrix

1. Assess risk ratings based on first selecting the relevant Consequence Criteria and level of severity, followed by the Likelihood Rating.
2. Use the *Risk Acceptance and Escalation Table* to evaluate the risk and determine which path to take to manage the risk (e.g. accept, monitor, treat).

| | CONSEQUENCE | | | | |
|---|---|---|---|---|---|
| LIKELIHOOD | Negligible | Minor | Moderate | Major | Severe |
| Almost Certain | Medium | Medium | High | Extreme | Extreme |
| Likely | Medium | Medium | Medium | High | Extreme |
| Possible | Low | Medium | Medium | High | High |
| Unlikely | Low | Low | Medium | Medium | High |
| Rare | Low | Low | Low | Medium | Medium |

# Risk Matrix

**NOTE:** the assessment of a risk occuring (likelihood) or the impact of an event (consequence) can be subject to personal bias. For this reason every step in the assessment requires communication and consultation. Risk Management best practice is that assessments are collaborative exercises best undertaken in a stakeholder risk workshop.

| RISK TOLERANCE | | |
|---|---|---|
| CATEGORY | | UPPER RISK THRESHOLD |
| Service, Delivery and Performance | Refer to Risk Appetite Statement | Medium |
| Capability and Resources | | Medium |
| Security | | Medium |
| Compliance, Governance and Integrity | | Low |
| Safety | | Low |

| LIKELIHOOD RATING | | |
|---|---|---|
| DESCRIPTOR | QUALITATIVE | PROBABILITY |
| Almost Certain | It is almost certain that the event or described result will occur. | 91% and above |
| Likely | A strong possibility that the event or described result will occur. | 61-90% |
| Possible | The event or described result could occur. | 31-60% |
| Unlikely | It is unlikely that the event or described result will occur. | 5-30% |
| Rare | The event may occur but only in rare and exceptional circumstances. | Less than 5% |

AEC Australian Electoral Commission

# Consequence Criteria

**Instructions for using consequence criteria:** Select the highest credible consequence. If your risk event occurred, which of the following criteria would apply?

| | Consequences | | | | | | |
|---|---|---|---|---|---|---|---|
| SCALE | SERVICE DELIVERY | FINANCIAL | PRIVACY | COMPLIANCE | REPUTATION AND IMAGE | FRAUD | WORK HEALTH AND SAFETY (WHS) |
| Negligible | Outcomes and objectives are substantially met. Minor delays in performance have no or little impact on delivery of business processes.<br>No measurable operational impact to ICT services. | Total dollar loss and/or potential overspend is less than or equal to $50,000 | Information is already in the public domain. No loss of public confidence | Minor technical breach of an internal policy or guideline. | Incidental media coverage. Little, if any, impact on stakeholder confidence. | Not Applicable | Injury to workers or other parties may require the attention of first aid officer. Comcare not notified. |
| Minor | Outcomes and objectives are substantially met with partial delay or variation. Some interruptions in performance having a minor and temporary impact on business delivery of processes.<br>Minor downtime or outage in single area of agency. Minimal loss of data. | Total dollar loss and/or potential overspend is greater than $50,000 and less than or equal to $1 million. | Small number of individuals affected and limited (non-sensitive) information involved (e.g. name, contact details, email). Limited risk of harm to small number of individuals including financial/reputational risk. | Failure to comply with internal policy and legislation. Accountable Authority Instructions (AAI), resulting in a minor breach of Commonwealth Acts, including the Commonwealth Electoral Act (CEA). | Isolated media coverage, limited to local media. Isolated or minimal impact to stakeholder confidence. Can be resolved within a short timeframe. | Isolated incident, may result in minor disciplinary action | One-off or near miss Work Health and Safety incident occurs. Only minor injury, if any, to workers or other parties. May require the action of a medical doctor. Comcare not notified. |
| Moderate | Delivery of key outcomes and objectives substantially delayed or varied. Some interruptions to time critical service delivery. Extended period of downtime or outage in multiple services. | Total dollar loss and/or potential overspend is greater than $1 million and less than or equal to $5 million. | Large number of individuals affected, with limited release of additional information to what is already in the public domain. | A breach of Commonwealth Acts or Regulations or failure to comply with PGPA Act, CEA and the Public Service Act. | Strong media interest. Moderate or broader damage to stakeholder confidence with short to medium outcomes and ramifications. Requires Executive attention. | Fraudulent activities resulting in disciplinary actions. | Multiple Work Health and Safety near miss incidents. Potentially a notifiable incident to Comcare under WHS Act. Medical treatment required for workers or other parties; and/or a dangerous incident as defined under the WHS Act (section 37). |
| Major | Unable to deliver outcomes without significant additional expense and/or variation. Breakdown in time-critical services. | Total dollar loss and/or potential overspend is greater than $5 million and less than or equal to $20 million | Risk of harm to large number of individuals including financial/reputational damage, or any release of sensitive information (e.g. silent electors, criminal records, health information, sexual orientation, TFNs).<br>Public exposure of incident and limited loss of public confidence. | Multiple breaches of Commonwealth Acts or Regulations with possible penalties under the CEA and Public Services Act. | Intense media attention with potential national coverage over current and future outcomes.<br>Widespread impact to stakeholders. Longer term impact to stakeholder perceptions.<br>Public perception severely damaged - considerable resources required to recover. | Clear, wilful fraudulent activities resulting in disciplinary actions with referral to the AFP. | Life threatening or a serious injury causing hospitalisation. A notifiable incident to Comcare under section 36 of the WHS Act. Major injuries of workers or other parties. |
| Severe | Unable to deliver outcomes in the foreseeable future. Unable to undertake time-critical and other services for a prolonged period.<br>Extensive and/or total loss of service delivery. | Total dollar loss and/or potential overspend is greater than $20 million. | Serious risk of harm to large number of individuals including financial and reputational risk and loss of sensitive information. Significant public exposure of issues and loss of public confidence. | Significant and or protracted breach of law resulting in criminal charges. | Extreme or hostile media attention over long term. Reputation and relationship with key stakeholders irrevocably damaged resulting in a material change in AEC's public perception. AEC is unable to obtain ongoing support. | Identified fraudulent activities resulting in disciplinary actions and reputational risk to AEC with referral to the AFP and termination of employment. | Preventable Death and/or major injuries on a significant scale. A notifiable incident to Comcare under WHS Act. |

AEC
Australian Electoral Commission

# Risk Acceptance and Escalation Table

1. **Determine which primary category the risk is related.**
2. **What is the residual risk rating?**
3. **What action is required?**

Once a risk has been identified and assessed, it must be evaluated to determine what further action is required. Actions may include accepting the risk; monitoring and maintaining existing controls; or escalating the risk with a Risk Treatment Plan and monitoring by an ELT member or governing committee.

The AEC has determined the agency's tolerance for risk based on our agency goals, strategies and operations. A risk is managed differently based on its assessed risk rating and risk category, as this affects whether the risk falls within or outside the agency's risk tolerance.

For example, a residual risk rated as 'Medium' would be considered acceptable if it related to the 'Capability & Resources' tolerance category, but would not be acceptable if it related to the 'Safety' tolerance category.

Use the *Risk Acceptance and Escalation Table* to determine if any action is required to treat or monitor a residual risk.

**Escalation level 1:** Develop a Risk Treatment Plan and escalate to an AC/SM. Risk to be reported to the Organisational Health Committee[1]

**Escalation level 2:** Develop a Risk Treatment Plan and escalate to an FAC, through the AC/SM. Risk to be reported to the Organisational Health Committee

**Escalation level 3:** Develop a Risk Treatment Plan and escalate to the DEC, through the AC/SM/FAC. Risk to be reported to the Organisational Health Committee and Executive Leadership Team

[1] For project risks, the Capability Committee will monitor any risks above tolerance, rather than the Organisational Health Committee.

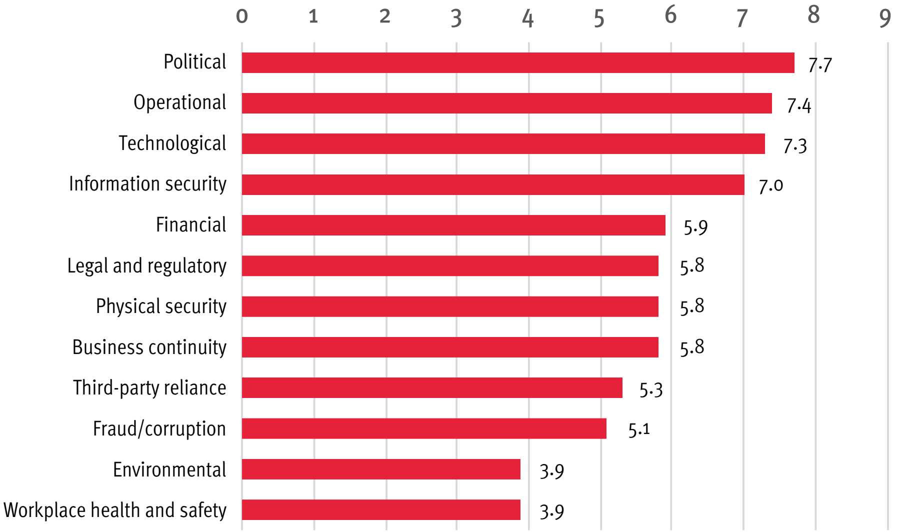
| | ESCALATION TABLE | | | | |
|---|---|---|---|---|---|
| **Residual Risk Level** | **Service, Delivery and Performance** | **Capability and Resources** | **Security** | **Compliance Governance and Integrity** | **Safety** |
| LOW | **ACCEPT**<br>Monitor control operations | **ACCEPT**<br>Monitor control operations | **ACCEPT**<br>Monitor control operations | **ACCEPT**<br>Monitor control operations | **ACCEPT**<br>Monitor control operations |
| MEDIUM | **ACCEPT**<br>Monitor control operations | **ACCEPT**<br>Monitor control operations | **ACCEPT**<br>Monitor control operations | ESCALATION LEVEL 1 | ESCALATION LEVEL 1 |
| HIGH | ESCALATION LEVEL 1 | ESCALATION LEVEL 1 | ESCALATION LEVEL 1 | ESCALATION LEVEL 2 | ESCALATION LEVEL 2 |
| EXTREME | ESCALATION LEVEL 2 | ESCALATION LEVEL 2 | ESCALATION LEVEL 2 | ESCALATION LEVEL 3 | ESCALATION LEVEL 3 |

AEC
Australian Electoral Commission

# Annex E. Key risks faced by electoral management bodies

According to the AEC and International IDEA 2019–2020 survey, to which 43 EMBs responded, the most prominent risks faced by EMBs are outlined in the table below.

Respondents were asked to select and rank 5–10 risks that are most relevant to their context, with a ranking of 1 indicating the risk of being most relevant. The weighted average of the responses was then calculated using the formula (x1w1+x2w2+x3w3…xnwn)/total. A higher score indicates a risk being more relevant.



| Risks based on ranking | Content of risk | Score |
|---|---|---|
| Political | Political environment is highly polarized and hostile during elections; political pressures; political consensus hard to reach; lack of trust | 7.7 |
| Operational | Lack of capability; insufficient number of staff; logistical challenges; potential for human errors; multiplicity of stakeholders involved | 7.4 |
| Technological | Exposure to technology failures; lack of trust in use of new technologies; security against external interfaces | 7.3 |
| Information security | Cyberattacks | 7.0 |
| Financial | Limited and inadequate finances | 5.9 |
| Legal and regulatory | Legal amendments close to an election; contractual issues (insurance, employments, rent, lease, construction, etc.); liabilities in case of property damage; environment protection | 5.8 |
| Physical security | Security of election officials, candidates, participants in electoral events and election materials | 5.8 |
| Business continuity | Interruption due to unforeseen events | 5.8 |
| Third-party reliance | Dependency on vendors, such as for providing IT services, data management, logistics | 5.3 |
| Fraud/corruption | Fraud, corruption, bribery, vote-buying | 5.1 |
| Environmental | Natural disasters, weather events | 3.9 |
| Workplace health and safety | Long working hours | 3.9 |

# Annex F. Elections Canada: risk assessment criteria and risk register

The information in this annex is published with the kind permission of Elections Canada. The risk assessment criteria and the risk register are not publicly available.

**Risk Assessment Criteria**

| LEVEL | PROBABILITY | IMPACT |
|---|---|---|
| Very high | • There is a greater than 90% chance that the risk will occur<br>• The risk has materialized often in the past under similar circumstances<br>• There is a consensus that the risk will most likely occur based on expert judgement<br>• "If I had to bet, I'm certain that it will occur" | • Very significant schedule slippage for a major commitment that cannot be accommodated; no workaround<br>• Very significant increase in costs; very significant knowledge, skill, and resources required<br>• Impact is felt across HQ and all electoral districts<br>• A critical component of a commitment will not be delivered; severely compromises ability to deliver an electoral event<br>• The impact will likely be perceived as unacceptable to Canadians<br>• The risk event would gravely affect more than one program or the reputation of EC |
| High | • There is a 65% to 90% chance that the risk will occur<br>• The risk has materialized in the past under similar circumstances<br>• There is a consensus that the risk will likely occur based on expert judgement<br>• "If I had to bet, I'm fairly certain that it will occur" | • Significant schedule slippage for a major commitment that cannot be accommodated; no workaround<br>• Significant increase in costs; significant knowledge, skill, and resources required<br>• Impact is felt across HQ and at least half electoral districts<br>• An important component of a commitments will not be delivered; compromises ability to deliver an electoral event<br>• The impact will likely be perceived as unacceptable to the organization<br>• The risk event would affect at least one program or the reputation of EC |

Risk Assessment Criteria

| LEVEL | PROBABILITY | IMPACT |
|---|---|---|
| Moderate | • There is a 35% to 64% chance that the risk will occur<br>• The risk may have materialized in the past under similar circumstances<br>• There is a consensus that, while not an absolute certainty that the risk occurs, there is cause for concern<br>• "If I had to bet, I'm fairly certain that there is a 50-50 chance that it will occur" | • Schedule slippage for a major commitment that cannot be accommodated; may be able to identify a workaround<br>• Increase in costs; significant knowledge/skill or significant resources required<br>• Impact is felt across HQ and possibly some electoral districts<br>• All critical or important components of commitment will be delivered; some non-critical component(s) of scope will be jeopardized<br>• The impact will likely be perceived as undesirable but manageable to the organization |
| Low | • There is a 10% to 34% chance that the risk will occur<br>• The risk has not, to our knowledge, occurred in the past under similar circumstances<br>• There is a consensus that the risk is unlikely to occur based on expert judgement<br>• "If I had to bet, I'm reasonably confident that it won't occur" | • Minor schedule slippage for a major commitment that can be accommodated; workaround available<br>• Minor impact on costs; limited knowledge/skill and resources required<br>• Impact is felt across HQ<br>• All critical or important components of scope will be delivered; some non-critical component(s) of scope may be jeopardized<br>• The impact will likely be perceived as acceptable to the organization |
| Very low | • There is less than a 10% chance that the risk will occur<br>• The risk has never occurred in the past under similar circumstances<br>• The risk will not occur, barring exceptional circumstances<br>• There is a consensus that the risk is extremely unlikely to occur based on expert judgement<br>• "If I had to bet, I'm confident that it won't occur" | • Little or no schedule slippage that can easily be accommodated; workaround readily available<br>• No significant impact on cost or scope, very limited skills, knowledge, or resources required<br>• Impact is felt across only part of HQ<br>• The impact will likely be perceived as insignificant to the organization |

## Example of Elections Canada's Integrated Risk Register

A **risk register** is a tool in risk management and project management. It is used to identify potential risks in a project or an organization, sometimes to fulfil regulatory compliance, but mostly to stay on top of potential issues that can derail intended outcomes.

The risk register includes all information about each identified risk, such as the nature of that risk, level of risk, who owns it, and any mitigation measures in place to respond to it.

Elections Canada captures corporate, programme and readiness risks and updates these in the Integrated Risk Register on a quarterly or bi-annual basis, and monitors them in accordance with the Risk Management Framework. This approach enables the agency to better coordinate risk management activities and responses across the organization, and provides the agency with a comprehensive view of its overall risk profile. Project risks are tracked and managed separately by the project leads.

| IDENTIFICATION | | | | | | | | | | RESPONSE STRATEGY | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Risk ID | Risk Category | Programme/Subprogramme | Oversight | Internal (ECHQ and Field) or External (Third-Party Partners) | Status | Risks Identified by OPIs/SMEs | Risk Owner(s) | Last Update: Date | Last Update: Additions | Risk Stakeholder(s) | Response Strategy/Action Plan | Action Plan Status | Deliverables & Milestone | Probability | Impact | Residual Risk |
| 8 | Corporate | N/A | SMC | Internal/ External | Ongoing | There is a risk that the demands created by electoral preparation in a minority government context can hinder the agency's ability to deliver on longer-term strategies, thereby limiting the agency's ability to meet the needs of Canadians. | CEO | Nov. 2020 | SMC meeting<br>Residual Risk remains high<br>Mitigation plan is on track. Action plans for GE and corporate pandemic response complete. | All Sectors | **MITIGATE**<br>Digital Strategy will address this risk going forward.<br>In addition to the Digital Strategy the agency will:<br>-Maintain focus on two tracks (short-term readiness activity, long-term strategy);<br>-Decouple projects from the electoral cycle with dedicated teams that follow a strict prioritization of projects;<br>-Adjust the cadence of activities;<br>-Renew corporate governance; and<br>-Draft a departmental investment plan. | Complete | Project prioritization approach.<br>Departmental investment plan. | Moderate | High | High |
| 16 | Programme | Regulatory Affairs—Electoral Integrity and Regulatory Oversight | Owner | External | Ongoing | There is a risk that false or misleading information about when, where and ways to register or vote will be shared, resulting in a compromise to electors' ability to access voting. | Senior Director, IRPPA | Jan. 2021 | Q3 Risk Review<br>Residual Risk remains moderate<br>Monitor continues to be the appropriate strategy | -PPA<br>-Legal<br>-Security<br>-OFG | **MONITOR**<br>Procedures and practices already in place are sufficient at this time. Monitor for change in environment that indicates a need for additional measures. | | | High | Low | Moderate |
| 56 | Programme | Regulatory Affairs—Political Financing | Owner | Internal | Ongoing | There is a risk that the Regulatory Affairs branch will see the departure of a number of employees with specific skill sets, resulting in a less experienced workforce which could prevent EC from achieving its goals with regard to completing GE43 activities and initiating GE44 activities. | DCEO, RA | Jan. 2021 | Q3 Risk Review<br>Residual Risk remains high<br>Mitigate continues to be the appropriate strategy. Implementation of mitigation plan is delayed. New activities are required to further mitigate this risk | -RA | **MITIGATE**<br>Agency will:<br>- Invest in talent management;<br>- Create a strengths matrix to identify strengths within the Political Financing Branch;<br>- Develop a succession plan;<br>- Strengthen the integration of the activities to diversify knowledge and experience;<br>- Use the Centre of Expertise to support new employees; and<br>- Continue internal training programme. | Requires Attention | Strengths matrix.<br>Succession plan. | High | High | High |
| 79 | Readiness/ Event Risk | All programmes | ORC | Internal/ External | Ongoing | **Electoral Materials**<br>There is a risk that not all electoral materials will be in stock or ready to ship in time for a snap election, resulting in ROs not having the required supplies to deliver services. | Senior Director, OFG and Director, OSS | Jan. 2021 | Q3 Risk Review (based on winter 2021 readiness vulnerability assessment)<br>Residual Risk remains low | -EEI | **ACCEPT**<br>The following strategies already in place are sufficient to address the risk:<br>- Minimize the number of changes to election materials.<br>- Start assembly for GE44 early and postpone sorting activities for GE43 until after the completion of GE44 assembly.<br>- Send PDF versions of documents to ROs for local printing. | | | Low | Low | Low |

| IDENTIFICATION | | | | | | | | | | | RESPONSE STRATEGY | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Risk ID | Risk Category | Programme/Subprogramme | Oversight | Internal (ECHQ and Field) or External (Third-Party Partners) | Status | Risks Identified by OPIs/SMEs | Risk Owner(s) | Last Update: Date | Last Update: Additions | Risk Stakeholder(s) | Response Strategy/Action Plan | Action Plan Status | Deliverables & Milestone | Probability | Impact | Residual Risk |
| 87 | Programme | Regulatory Affairs—Electoral Integrity | Owner | External | Ongoing | There is a risk that facing a pandemic outbreak during a writ period, prominent actors will call for the Chief Electoral Officer (CEO) to recommend postponing election day or withdrawing the writ, claiming that holding an election in such circumstances diminishes its legitimacy. | DCEO, RA | Jan. 2021 | Q3 Risk Review<br>Residual Risk remains high<br>Mitigation plan on track | -RA<br>-PACE | **MITIGATE**<br>Agency will:<br>- Prepare a strategic communications plan for use if issue is detected; and<br>- In the longer term, consider developing a policy instrument to set guidelines for the use of section 59 of the CEA. | On track | Strategic communications plan<br>Draft messages and media lines<br>Policy on use of S. 59 | High | Moderate | High |
| 94 | Programme | Public Affairs and Civic Education | Owner | External | Closed | There is a risk that all Voter Information Campaign products may not be updated to reflect new legislative changes if election is called within a few days of legislation measures coming into effect, leading to Canadians receiving incorrect information. | Executive Director, PPA | Oct. 20 | All material now ready | -PACE | | | | | | |
| 104 | Programme | Electoral Events and Innovation | Owner | Internal | Ongoing | There is a risk that due to the pandemic it will be more difficult to put HR strategies in place, and, as a result, we may not be able to hire all the staff required to deliver an election. | DCEO, EEI | Jan. 2021 | Q3 Risk Review<br>Residual Risk remains high<br>Mitigation plan on track | -EEI | **MITIGATE**<br>Agency will:<br>- Ensure staffing pools are ready;<br>- Have online training available for employees;<br>- Develop a strategy and plan to keep employees motivated and maintain morale;<br>- Continue to equip employees properly to work from home; and<br>- EEI to meet with HR every two weeks to ensure implementation remains on track. | On track | Staffing pools.<br>Online training.<br>Motivational plan<br>Work from home plan, instructions, equipment | High | High | High |

# Annex G. IEBC Kenya: risk matrix, risk register template and heat map

The information in this annex is published with the kind permission of the Independent Electoral and Boundaries Commission of Kenya. The risk matrix, risk register template and heat map are not publicly available.

## Risk matrix

| Risk category | Risk | Mitigation measures | Risk owner |
|---|---|---|---|
| **Legal risks** | i. Delay in enactment or amendments of electoral law<br>ii. Last-minute amendment of laws<br>iii. Lack of timely interpretation of the laws<br>iv. Judicial rulings that affect the election timelines | i. Engagement with parliament and stakeholders<br>ii. Seek legal opinion of the Attorney General<br>iii. Timely legal interpretation<br>iv. Compliance with the law<br>v. Appeal of cases | Commissioners<br>DLPA |
| | Delayed enactment of referendum laws and regulations | Engage parliament to enact the relevant laws | Commissioners<br>DLPA |
| **Political risks** | i. Refusal to accept election results | i. Have contingency plans to respond to emerging issues<br>ii. Conduct continuous risk assessments | Commissioners<br>DARC |
| **Strategic risks** | i. Constitution of the Commission<br>ii. Replacement of commissioners too close to the election | i. Engage Parliament on timely replacement of commissioners | Chairperson of the Commission |

| Risk category | Risk | Mitigation measures | Risk owner |
|---|---|---|---|
| **Financial risks** | i. Non-operationalization of the IEBC Fund<br>ii. Inadequate budgetary provision<br>iii. Delayed Exchequer release | i. Operationalizing the IEBC Fund<br>ii. Engage Parliament and Treasury for financing of planned activities<br>iii. Budgeting to be aligned with Commission's core mandate<br>iv. Early requisition of Exchequer | Commissioners<br>CEO<br>DF |
| | Pending bills | Engage Treasury for allocation of funds to clear pending bills | CEO<br>DF |
| **Technological risks** | Malfunctioning of ICT systems and equipment | i. Maintenance and testing of ICT equipment and systems<br>ii. Upgrading of ICT systems and equipment | DICT |
| | Overreliance on third-party platforms | i. Skills transfer to Commission staff<br>ii. Timely funding and adequate time for implementation of ICT systems | DLPA<br>DICT |
| | Over-legislation on use of ICT | Review of the law | DICT<br>DLPA |
| | Cybersecurity threats | Enhance ICT security system | DICT |
| | Centralization of ICT procurement in the Ministry of ICT | i. Engage Treasury to exempt the Commission from the directive and allow its autonomy in ICT procurement<br>ii. Direct engagement with the Office of the Attorney General | Commissioners<br>CEO<br>DSCM<br>DICT |
| | Obsolescence of BVR kits | Modify KIEMs to perform registration function | DICT |

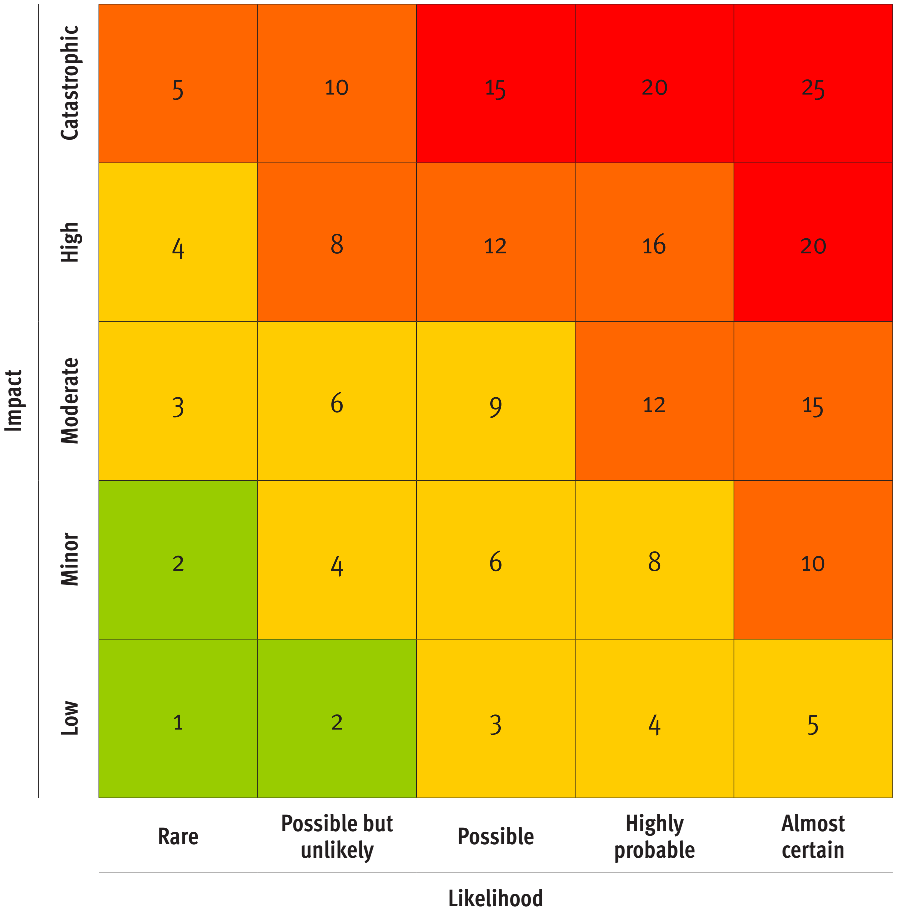
| Risk category | Risk | Mitigation measures | Risk owner |
|---|---|---|---|
| **Operational risks** | Delay in procurement of strategic and non-strategic election materials | i. Enter into framework agreements with service providers<br>ii. Early requisition of materials | CEO<br>DSCM |
| | Low voter registration turnout | i. Engage stakeholders in mobilization of eligible voters<br>ii. Conduct continuous voter education for voter registration<br>iii. Adequate facilitation of voter registration and education<br>iv. Targeted voter registration | DVREO<br>DVEPC<br>DF |
| | Insecurity during electoral activities | i. Establish an election security plan with security agencies<br>ii. Enforcement of electoral code of conduct | Commissioners<br>CEO<br>DLPA<br>DARC<br>DHRA |
| | Profiling of IEBC staff | i. Enhance security for staff<br>ii. Engage with stakeholders | DHRA<br>DARC |
| | High staff attrition | i. Improved staff welfare and security<br>ii. Institute career progression<br>iii. Establish a staff reward mechanism | DHRA |
| | i. Under remuneration of temporary poll officials<br>ii. Occupational hazards such as accidents suffered by temporary poll officials | i. Improve the terms of service for temporary poll officials including accommodation during training in vast constituencies | DHRA<br>DF |

| Risk category | Risk | Mitigation measures | Risk owner |
|---|---|---|---|
| **Reputational risks** | Negative publicity and reduced public trust | i. Engage media and stakeholders during electoral activities<br>ii. Enhance public sensitization on Commission activities<br>iii. Enhance transparency in Commission operations | Commissioners<br>DVEPC<br>CEO |
| **Compliance risks** | Non-compliance with policies, laws, procedures and obligations | Sensitize staff and enforce the relevant legislations, policies, procedures and obligations | Commissioners<br>CEO<br>All Directors |

## Risk register template

| | | | |
|---|---|---|---|
| **Risk No.** | | | |
| **Risk description** | | | |
| **Risk event** | | | |
| **Risk source/cause** | | | |
| **Key risk indicators (KRI)** | | | |
| **Consequences** | | | |
| **Probability rating** | | | |
| **Impact rating** | | | |
| **Overall risk rating** | | | |
| **Treatment strategy** | | | |
| **Risk owner** | | | |
| **Date of posting** | | | |
| **Comments as at XX—XX-XXXX** | | | |

## Heat map



| Impact | Rare | Possible but unlikely | Possible | Highly probable | Almost certain |
|---|---|---|---|---|---|
| Catastrophic | 5 | 10 | 15 | 20 | 25 |
| High | 4 | 8 | 12 | 16 | 20 |
| Moderate | 3 | 6 | 9 | 12 | 15 |
| Minor | 2 | 4 | 6 | 8 | 10 |
| Low | 1 | 2 | 3 | 4 | 5 |
|  | Likelihood |  |  |  |  |

# About the authors

**Amy Vincent** has acquired considerable knowledge and experience in financial management, assurance, risk management and resilience-building through a career spanning nearly 20 years across the Australian public and private sectors in business continuity management. Her professional roles have included management accounting, auditing, governance and enterprise risk advisory. She is currently a Senior Manager at Deloitte Consulting, previously Director, Governance and Performance Advisory at the Australian Electoral Commission.

**Sead Alihodžić** is a Senior Advisor at International IDEA with over 20 years of experience in managing a broad portfolio of election-related topics, including electoral risk management and resilience-building, the conduct of elections in transitional contexts, and electoral conflict and violence prevention. He led the design and development of International IDEA's Electoral Risk Management Tool, managed several related technical assistance projects implemented worldwide and has acted as lead author of International IDEA guides and policy papers. He has also contributed to external journals and publications.

**Stephen Gale** has worked across a number of Australian commonwealth agencies and has skills in governance and reporting roles (including risk management, project management and lessons management), and developing and delivering training and facilitation exercises. At the Australian Electoral Commission, he is currently Acting Director, Governance and Performance Advisory, with responsibility for risk management and other governance functions.

# About the partners

## Australian Electoral Commission

The Australian Electoral Commission (AEC) conducts federal elections and referendums and maintains the Commonwealth Electoral Roll. It is an independent, statutory authority responsible for administering the Commonwealth Electoral Act 1918 and the Referendum (Machinery Provisions) Act 1984.

### What do we do?

The AEC is responsible for maintaining an impartial and independent electoral system for eligible voters through active electoral roll management, efficient delivery of polling services and targeted education and public awareness programmes. The AEC achieves this by:

- conducting successful electoral events, including federal elections, by-elections and referendums, and industrial elections and ballot programmes;
- ensuring confidence in the electoral roll;
- regulating political party registrations and financial disclosure;
- supporting electoral redistributions; and
- undertaking public awareness activities.

The AEC's vision is to become a leader in refining and delivering best practice in election management.

The AEC also provides a range of electoral information and education programmes, both in Australia and in support of Australia's national interests.

### Where do we work?

The AEC has a national office in the Australian capital, Canberra, with state and territory offices and divisional offices.

## International IDEA

The International Institute for Democracy and Electoral Assistance (International IDEA) is an intergovernmental organization with the mission to advance democracy worldwide, as a universal human aspiration and enabler of sustainable development. We do this by supporting the building, strengthening and safeguarding of democratic political institutions and processes at all levels. Our vision is a world in which democratic processes, actors and institutions are inclusive and accountable and deliver sustainable development to all.

### What do we do?

In our work we focus on three main impact areas: electoral processes; constitution-building processes; and political participation and representation. The themes of gender and inclusion, conflict sensitivity and sustainable development are mainstreamed across all our areas of work.

International IDEA provides analyses of global and regional democratic trends; produces comparative knowledge on democratic practices; offers technical assistance and capacity-building on reform to actors engaged in democratic processes; and convenes dialogue on issues relevant to the public debate on democracy and democracy building.

### Where do we work?

Our headquarters are located in Stockholm, and we have regional and country offices in Africa, Asia and the Pacific, Europe, and Latin America and the Caribbean. International IDEA is a Permanent Observer to the United Nations and is accredited to European Union institutions.

<https://www.idea.int>

When electoral risks are not understood and addressed, they can undermine the credibility of the electoral process and the results it yields. Electoral management bodies (EMBs) encounter numerous risks across all phases of the electoral cycle. They operate in environments that are increasingly complex and volatile and where factors such as technology, demographics, insecurity, inaccurate or incomplete information and natural calamities create increasing uncertainty.

The experiences of EMBs show that when formal risk management processes are successfully implemented, the benefits are profound. Greater risk awareness helps organizations to focus their resources on where they are most needed, thus achieving cost-effectiveness. Over the last decade it has been observed that EMBs are increasingly moving from informal to formal risk management processes.

The purpose of this Guide is to lay out a set of practical steps for EMBs on how to establish or advance their risk management framework. The Guide's chapters reflect the breadth of key considerations in the implementation process and offer basic resources to assist in the process.

**International IDEA**
Strömsborg
SE–103 34 Stockholm
Sweden
Telephone: +46 8 698 37 00
Email: info@idea.int
Website: <https://www.idea.int>

ISBN: 978-91-7671-437-9 (Print)
ISBN: 978-91-7671-438-6 (PDF)