INTOSAI IDI DEVELOPMENT INITIATIVE

Well-Governed SAIs WORK STREAM

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Economic Affairs SECO

Risk Management for Supreme Audit Institutions

Quick Reference Guide

December 2023

CRISP Crisis and Risk Management for SAI Performance

AN INITIATIVE
COVERING RISK AND CRISIS MANAGEMENT
FOR SAI PERFORMANCE

CONTENTS

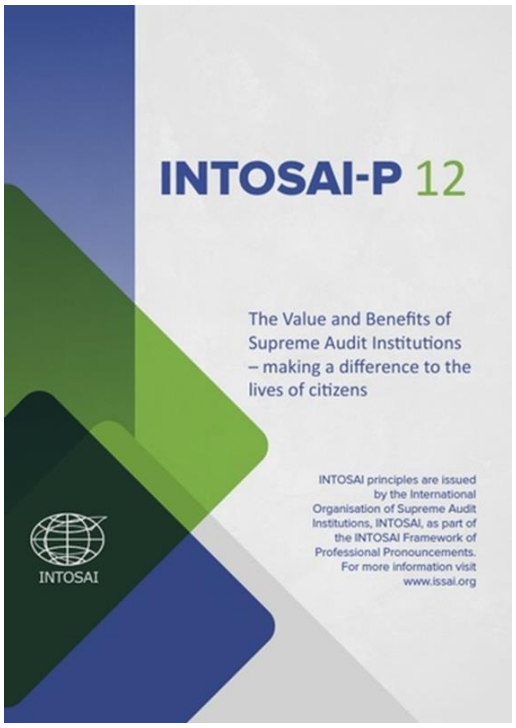
CRISP Crisis and Risk Management for SAI Performance

The importance of risk management

Risk management is a condition to SAI performance and as such supports a robust strategy and effective operational plan

Like any other private or public organisation, Supreme Audit Institutions (SAI) are not immune from disruption and are exposed to risks. The INTOSAI Development Initiative Global SAI Stocktaking Report 2020 shows evidence of this: '*Globally, 53% of SAIs have an emergency preparedness and continuity plan. Lower income countries are significantly lagging behind the higher income countries*.'

While SAIs routinely evaluate changing and emerging risks in the audit environment, it appears that a substantial proportion of them do not do this for their own strategy and operations which is a key requirement of INTOSAI-P 12.



Being a model organization through leading by example

Principle 9:
Ensuring good governance of SAIs

4) SAIs should assess organizational risk on a regular basis and supplement this with appropriately implemented and regularly monitored risk management initiatives, for example through an appropriately objective internal audit function.

The SAI strategy and the operational plan are based on assumptions, so it is important that they are designed considering the risks they entail. Doing so, the SAI will be better prepared. This will build the SAI resilience and further improve its performance.

CRISP Crisis and Risk Management for SAI Performance

The goal is to reduce the likelihood and impact of negative events, lost opportunities, and surprises and increase the probability that the objectives of the SAI will be met to maximize its performance.

Managing risk requires the implementation of a dedicated methodology. IDI approach is based on ISO 31000:2018 Risk Management Guidelines.

This Quick Reference Guide introduces the main tools that SAIs can use to develop and implement their risk management.

IDI also offers a full-fledged training that explains in detail the risk management methodology and can also provide tailored support for those SAIs who require specific assistance.

The IDI CRISP Team can be contacted at crisp@idi.no

The risk management policy

The starting point of risk management is to develop and approve a risk management policy

IDI has developed a template for SAIs to refer to when they build their risk management policy. This template has 14 components which together will form a comprehensive and robust risk management policy and is filled with examples of real policies developed by SAIs for a better understanding of the content and guidance (see Appendix A).

- Purpose
- Scope
- General principles
- Risk Governance
- Risk Management Process
- Integration with our systems and processes
- Risk Categories
- Risk Register
- Risk Reporting
- Risk Management Performance
- Risk Appetite
- Significant Risks
- Review and Approval
- References and related documents

Risk identification and assessment

The next step is to identify and assess risks

Risk identification

The purpose of risk identification is to find, recognize and describe risks that might help or prevent an SAI achieving its objectives.

This is done within a defined scope which specifies the extent of coverage in the parameters of the SAI's internal & external vulnerabilities. The scope takes into consideration the different result levels, expected outcomes, the time frame (usually the strategic plan/operational plan period) and the SAI capacity.

Risk assessment

The purpose of risk assessment is to comprehend the nature of risk and its characteristics including, where appropriate, the level of risk.

This template is based on a 5 levels rating system for likelihood and consequences. This can be adapted to fit the SAI specific needs and approach (e.g., a 3 or 4 levels rating system. It is not advisable to have too many levels).

Rating risk likelihood

Relative	Description	Percentage	Weight
Near certain	Highly likely to occur	91 – 100 %	5
Likely	Likely to occur	61 – 90 %	4
Moderate	Possible to occur	41 – 60 %	3
Unlikely	Most like won't occur	11 – 40 %	2
Insignificant	Highly unlikely to occur	0 – 10 %	1

The likelihood is determined based on past experiences and events or expectations during the coming periods based on developments surrounding the SAI.

Rating risk consequences

Relative	Criteria	Weight
Catastrophic	✓ Highly disruptive to the SAI ✓ Extended legal consequences that threaten the SAI's existence	5
Major	✓ Substantiated public embarrassment with a high news profile ✓ Reason to extended legal scrutiny of the SAI with the possibility of criminal charges	4
Moderate	✓ Substantiated public embarrassment ✓ Substantiated legal violations, subject to fines or penalties	3
Minor	✓ Substantiated consequences for the SAI ✓ Moderate legal violations that can be quickly corrected	2
Insignificant	✓ Consequences can be quickly contained and recovered ✓ Minimal legal violations	1

The consequences are determined based on previous experiences and events or expectations during the coming periods based on the developments surrounding the unit.

The combination of ratings will provide the criticality of the risk:

Criticality (likelihood x impact)		Action priority
1-4	Low criticality	Low priority. No immediate further action required
5-10	Moderate criticality	Moderate priority. Monitor the risk without any immediate further action
12-16	High criticality	High priority. Take necessary mitigation action
20-25	Extreme criticality	Very high priority. Take necessary mitigation action, report to Management, keep under continuous monitoring.

The risks can then be presented together in a heat map where each risk is placed according to its criticality:

Impact	Likelihood				
	Insignificant	Unlikely	Moderate	Likely	Near to certain
Catastrophic	5	10	15	20	25
Major	4	8	12	16	20
Moderate	3	6	9	12	15
Minor	2	4	6	8	10
Insignificant	1	2	3	4	5

While assessing criticality is important, SAIs need to decide on the risks they want to prioritize because it is not possible to treat them all at the same time. At this stage, it is key to assess the faculty of action or the ability of the SAI to react to the identified risk:

Weight	Criteria	Relative
3	This would mean that the SAI has not done anything or very little to manage this risk. This is usually the case for risks that have newly emerged. On the other and this applies to risks, for which the SAI possesses a real ability to control.	High
2	There is significant room for improvement in managing this risk, meaning that the SAI could do much more. Usually, some processes have been developed by the SAI to mitigate but these have proven only partially effective or limit only aspects of the risk.	Significant
1	There is limited faculty of action concerning this risk. That means that the SAI already has many tools and processes in place and implements them but sees some room for improvement or perfection of these measures.	Limited
0	The SAI is not able to do anything further to control this risk. That would mean that all processes and tools the SAI could apply are already in place, or that all causes and consequences of this risk are beyond the influence of the SAI. It is unlikely that many risks would be categorized in this way unless the SAI has a very mature risk management process.	Null

Then, through combining criticality with faculty of action, SAI can identify the risk treatment priority. The highest faculty of action will increase the priority while a low faculty of action means that not much can be done, hence a low priority.

Through this analysis, the SAI will be able to focus its limited resource where it has the highest impact.

Risk treatment

Once risks have been identified and assessed, they need to be treated

Treating a specific risk may involve one or more of the following approaches:

- Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk
- Taking or increasing the risk to pursue an opportunity
- Removing the risk source
- Changing the likelihood
- Changing the consequences
- Sharing the risk
- Retaining the risk by informed decision

This will serve to build a risk treatment plan which will contain the following information:

- the proposed actions
- the reasons for selecting the treatment options and the benefits to be gained
- the resources required
- when actions are expected to be undertaken and completed
- Who is accountable and responsible for approving and implementing the plan
- the performance measures
- the constraints
- the required reporting and monitoring

Since all risks cannot be treated at the same time, the SAIs will need to prioritize. This is commonly done through assessing the faculty of action on the different risks.

IDI has developed a template for SAIs to register their risks together with their rating and treatment activities (see Appendix B).

The performance of the risk management process

The risk management process should be monitored, and reviewed and its outcomes need to be documented and reported

Monitoring (on an ongoing basis) and reviewing (on a periodic basis) the risk management process aim to ensure it is of sufficient quality (quality assurance) and effective.

Review and monitoring shall cover the different levels of the risk management procedure: Design, Implementation and Outcomes.

Recording and reporting on the risk management process allow the SAI to:

- Communicate risk management activities and outcomes across the SAI to support awareness, buy-in, building trust and support change management
- Provide information for decision-making
- Improve risk management activities: exposing the activities attract interest, hence ideas to improve the process
- Assist interaction with stakeholders, including those with responsibility and accountability for risk management activities: ensure buy-in, build trust in the capacity of the SAI to build its strategy and to implement it

IDI has developed a template for SAIs to report on their risk management (see Appendix C).

It is advisable to integrate risk management into the performance management cycle and performance reports. By incorporating risk management principles into performance evaluation processes, SAIs can better monitor progress towards strategy execution, enhance decision-making, and foster a risk-aware culture.

Appendices

- Appendix A - Risk Management Policy template
- Appendix B - Risk register template
- Appendix C - Risk management report template

Contact us

crisp@idi.no

CRISP Crisis and Risk Management for SAI Performance