

# General Internal Control and Risk Management Framework

Prepared by Andrew Graham, School of Policy Studies, Queen's University, Kingston, Ontario

In this context risk is defined as something adversely affecting the achievement of the agency's objectives or threatening compliance or reporting requirements. In a wider sense also lost opportunities are considered as risks.

Successful implementation of an internal control and risk management system as well as an assessment of the system depend on a clear and robust framework. The system must be down to earth, understandable and linked to the agency's planning and management system. In order to keep the system concise, it must prioritize material questions. It must also be linked to the organization's capacity to learn in a systematic way as well as communicate risk and risk mitigation activities both internally and externally. It must also be understood that the internal control extends well beyond the financial responsibilities of the organization and is linked directly to the objectives, outputs and anticipated outcomes of its activities.

Since internal control and risk management are not one-person-missions, top management must delegate tasks and responsibilities to lower management as well as have full support from the underlying organisation. Such delegation is facilitated by the use of common tools for internal control and risk management. Risk management only works, however, when the loop-back of accountability and consistent senior management engagement are sustained in a systematic way over time.

## Framework for internal control and risk management

This framework is meant to illustrative and provide direction. It is general in nature, based on the COSO<sup>1</sup> Enterprise Risk Management – Integrated Framework (COSO-ERM). Since, increasingly, public agencies are required either by law or policy to make an assessment of the status of their internal control and risk management systems, some generally accepted framework must be used.

Internal control and risk management should not be isolated from the normal management and planning process but rather be integrated to it. The objectives of internal control are to ensure:

- 1) the legality of the finances and operations of government agencies;
- 2) the results of the operations of government agencies relative to their stated objectives;
- 3) the security of the funds and assets managed by government agencies; and
- 4) the true and fair view of the finances and operations of government agencies required for each government agency's management and external steering.

---

<sup>1</sup> Committee of Sponsoring Organizations of the Treadway Commission

The internal control and risk management framework supports agencies in three ways:

1. the framework can be used as a tool when making the assessment required for the statutory assessment of internal control systems;
2. the framework serves as a communication and guidance tool to increase understanding of modern internal control and risk management methodology;
3. the framework can be used as a checklist to identify internal control areas requiring development.

In the framework, like in COSO-ERM, internal control is divided into eight components, which are:

1. Internal environment
2. Objective setting
3. Risk identification
4. Risk assessment
5. Risk response
6. Control activities
7. Information and communication, including organizational learning
8. Monitoring

Each of these components are divided into sub-areas in order to achieve a structured and scalable approach. In each sub-area one or more issues can be addressed when assessing the status of the internal control system of the agency.

The framework is a supporting tool only. Final assessment will be dependent on the organization's collective judgment, reflecting the many related issues associated with a robust and in-depth understanding of risk. The purpose of the framework is to guide the organisation and to ensure that evaluation of internal control and risk management follows a systematic and documented path and that all relevant components are included in the assessment.

Senior management of an agency has the responsibility of organizing the internal control of the agency. This responsibility is closely related to or even a sub-set of management's responsibility to strive towards achieving the agency's results, complying with statutes and reporting accurately. However, it is also the responsibility of those providing oversight to the agenda, be it a legislature, a governing board or body or a designated external auditor, to assure that systems of control are in place, that they are effective and that they produce the anticipated results.

The purpose of the statement is to

- emphasize senior management's responsibility for setting up and maintaining internal control and risk management systems;
- increase understanding of internal control and risk management among management and employees;
- support systematic and continuous development of internal control as part of management of the agency;
- report to the agency's supervisory body about the status of the agency's internal control and risk management systems; and
- increase public understanding and trust in the agency's activities.

All employees in the organization have the responsibility of maintaining a good internal environment, be aware of how internal control and risk management relate to their work and to report internal control issues to management. In particular, employees have a robust understanding of the operational processes of the organizational that could either place the organization at risk or quickly and effectively mitigate emerging risks. An organization ignores such insights at its peril.

Possible internal audit function has as its task to monitor the status of the internal control system and report on weaknesses in the system. Internal audit also acts as an internal control and risk management expert thereby supporting the internal learning process in the organization

## Governance, Policy and Oversight

SUB-AREA	ISSUE	REFERENCE	VERIFICATION	CONCLUSION
Policy Clearly Enunciated	The organization should articulate a strong commitment to a risk management policy.	General policy statement – general direction from oversight body or board, detailed process and management direction from senior management.	Adequate policy is in place and communicated.	
Governance roles understood and actively pursued	The different roles of the Board or other oversight body and CEO must be clearly delineated.	Oversight bodies provide broad direction. The CEO and senior management are responsible for responses to risks, managing the overall system and providing reports to the oversight body and engaging them in an appropriate way.	Oversight bodies provide policy direction. Adequate protocols exist to delineate the roles of the oversight body. CEO puts in place policies and practices to bring this to effect. CEO reports in a systematic way to the governing body or its designated sub-committee. The identification of risk and its mitigation are an integral part of the strategic planning process of the organization.	

## Internal environment

The internal environment of an organisation lays down the foundation for management's and employees' attitude to risks and controls. Internal environment is made up of risk appetite and tolerances and attitudes to internal control of senior management and supervising bodies and organizational personnel policy. Internal environment includes i.a. following areas: risk appetite of the organisation, honesty and ethical values, control principles, organizational structure, empowerment of employees, codes of conduct and know-how of employees.

SUB-AREA	ISSUE	REFERENCE	VERIFICATION	CONCLUSION
Internal culture	Management is committed and takes its responsibility	Policies and codes of conduct,	Management accepts plans and follow-up reports, gives and takes feedback and shows good example	
	Management has defined and communicated the organization's general risk approach including tolerances where possible and practical.	Strategies, risk management principles and policies.	As part of strategic planning management defines the types and amounts of risk that the organization can take in its operations. In addition, ways are indicated for verifying risk tolerances in unknown or emerging areas, including review by senior management	
	The organization has common ethical principles (or values), which members of the organization are aware of and act accordingly.	Ethical values, code of conduct, Civil servant ethics, personnel rules and guidelines, employee discussions.	Management communicates acceptable code of conduct and links it to all planning and decision making. Management reacts to unethical behaviour.	
	Members of the organization know	Acts laying down acceptable and	The organization has a systematic way	

	relevant rules and act according to them	required behaviour of civil servants	of communicating relevant rules to personnel. Non-compliance is dealt with systematically and fairly	
	The organizational culture promotes open discussion even about possible problems	Ethical values, agency financial rules, reporting rules, whistle blowing procedures, agency administration rules, personnel strategy	New suggestions and criticism is dealt with in a constructive way. Failure is tolerated. Employee satisfaction is good.	
	Incentives are rational and fair	Employee discussions, salary systems	Incentive systems are transparent, systematic and widely accepted.	
Organization	The organizational structure supports efficient operation	Organization chart, management system, agency administration rules, job descriptions	Tasks and responsibilities are clear. Organizational structure supports mission and strategy realization	
	Responsibilities, tasks and powers are clearly defined and communicated	Agency financial rules, management system, agency administration rules, job descriptions, employee discussions	Responsibilities and tasks are defined for all major areas	
Resources	Personnel has the knowledge required for their tasks <ul style="list-style-type: none"> <li>• efficient recruiting</li> <li>• evaluation of knowledge and skills</li> <li>• knowledge development</li> <li>• adequate amount of personnel</li> </ul>	Governing employment legislation, collective agreements, personnel strategy and policy, personnel and knowledge management plans.	The organization has documented and updated knowledge needs and resources. Personnel policies are communicated and complied with. Knowledge development is linked to operational needs	
	The organization has IT-systems that are required by its tasks	IT strategy, system descriptions, usability reports, archive rules, contingency plans	IT-systems supporting operations are reliable and documented. Data registration is systematic. Information is available	
	The organization has adequate infrastructure: premises, machines and services required by its mandate and objectives.	Strategy, budget, contingency plans	Projects and procurements are derived from strategies and are within the organizations financial resources.	

## Objective setting

In order to recognize relevant risks, the activities and objectives of the agency must be planned, monitored and steered.

SUB-AREA	ISSUE	REFERENCE	VERIFICATION	CONCLUSION
Mission and tasks	The organization has a clear mission. Management has defined vision and strategy.	Mission, vision, strategy	Mission and vision is the basis of all planning.	
	All members of the organization know its mission and way of action as well as the role and objectives of their own unit as part of the organization as a whole.	Strategy and its communication	Strategy is clear and to relevant parts known by everybody in the organization.	
	The organization has clear strategic objectives.	Strategy, financial and operational plans, planned results	The organisation has clear long-term strategic objectives, which support the organization's mission	
Planning	Operations are systematically planned	Budget act and decree, Agency financial	Strategy and plans derived from it are	

	and followed-up on all levels of the organization	rules, Result agreement, Planning guidelines, follow-up reports, annual reports	based on analysis of internal and external environment. Planning and follow-up is based on legal requirements and guidelines.	
	The organization has clear operational objectives	Planning documents	The organization has clear, relevant objectives for efficiency and effectiveness	
	The organization has clear reporting objectives	Planning documents	The organization has clear, relevant objectives for reporting	
	The organization has clear compliance objectives	Planning documents	The organization has clear, relevant objectives for compliance	
	Objectives are derived from upper level objectives and missions	Planning documents	Objectives are documented and form a hierarchy	
	Objectives are prioritized and scheduled as well as linked to indicators, action and resources.	Planning documents	All major operational areas are covered by objectives. All objectives are linked to one or more indicators	
	Objectives are efficiently communicated.	Communication plan, agency administration rules, job descriptions	Planning process is transparent and personnel is informed in a timely manner in order to enable them to participate in the planning process	

## Risk identification

Identification and documentation of events that may affect the achievement of the organization's objectives.

SUB-AREA	ISSUE	REFERENCE	VERIFICATION	CONCLUSION
Risk identification	Risk identification is systematic and ongoing	Risk management policy, planning documents, strategy and quality systems	Risk identification is based on a clear methodology. Identified risks are documented.	
	The organization regularly evaluates the impact of its external environment on its operations	Strategy systems (BSC), SWOT-analysis, stakeholder analysis, scenarios, changes in legislation	External factors, limitations and changes in these are considered in strategic planning.	
	Risk identification covers all parts of the organization as well as major projects	Risk management policy, project reporting, anomaly reports	The organization executes systematic risk identification. Risk management reports	
	Risk identification covers all types of objectives: <ul style="list-style-type: none"> <li>• strategic objectives</li> <li>• operational objectives</li> <li>• compliance objectives</li> <li>• reporting objectives</li> </ul>	Risk management policy, planning documents, anomaly reports	Risks affecting desired outcomes are identified, risks threatening operational objectives are identified, legal and other compliance risks are identified, risks threatening reliable internal and external reporting are identified	

	Risks affecting the achievement of objectives ( <i>strategic, operational, reporting, compliance, good governance</i> ) are identified as part of the planning process	Planning guidelines, planning documents, project plans	Risks are linked to objectives in planning documents	
--	--	--	--	--

### Risk assessment

Risks are analyzed considering the likelihood (probability) and impact (effect) of the events.

SUB-AREA	ISSUE	REFERENCE	VERIFICATION	CONCLUSION
Risk assessment	Identified risks are regularly analyzed	Risk management policy, planning documents	Risk assessments are documented	
	Material risks are analyzed extensively	Risk management policy, planning documents	All identified risks are analyzed or prioritized and material risks are analyzed	
	The likelihood and impact of risks are analyzed	Risk management policy, planning documents	Risk assessments are documented	
	Risk evaluation is objective but combines both quantitative and qualitative judgement.	Risk management policy	Assessments are based on quantitative data, external evaluations or extensive self assessments	
	Analyzed risks are reported to management	Risk reports, planning documents	Material risks are reported to management at all levels	
	Final risk assessments are subject to senior management approval.	Final risk assessment reports are approved by senior management.	Risk reports and assessments are not simply received, but either endorsed, modified or rejected.	

### Risk response

Evaluated risks will be related to the organization's risk appetite. Management will select response strategies (acceptance or risk management) based on cost-benefit analyzes.

SUB-AREA	ISSUE	REFERENCE	VERIFICATION	CONCLUSION
Risk classification	Analyzed risks are prioritized	Self assessments, risk management policy, risk reports	Management relates risks to organizational objectives and risk appetite	
	Risk responses are identified	Meeting minutes, risk management policy, risk reports	Prioritized risks are controlled by: i) avoiding; ii) reducing; iii) sharing; or iv) accepting the risks	
	Risk responses are based on cost/benefit –analysis	Meeting minutes, risk management policy	Costs of risk response is compared with benefits with reduced risks. Possible new risks caused by risk responses are evaluated	
	Management accepts selected risk responses	Meeting minutes, risk management policy	Clear management decisions on risk response including acceptance of risks.	
	Appropriate controls and responsibilities are defined for risks	Risk management policy	Documented controls	

## Control activities

Processes, procedures, structures or equipment that mitigate risks or increase opportunities. Control activities can be proactive or post-event activities decreasing the effect of the risk. Control activities should give reasonable assurance that the organization's objectives can be achieved.

SUB-AREA	ISSUE	REFERENCE	VERIFICATION	CONCLUSION
Planning of controls	Major operational processes are described together with associated risks and controls	Process descriptions, agency financial rules, policies and rules	Updated business process documentation	
	Controls cover: <ul style="list-style-type: none"> <li>operational and financial compliance</li> <li>effective and efficient operations</li> <li>safeguarding of assets</li> <li>reliable internal and external reporting</li> </ul>	Process descriptions, planning and follow-up documents, process quality reports, agency administrative rules, user rights and powers, asset registry	Business process documentation includes description of controls; the organization has a risk – control matrix.	
	Management makes decisions about control procedures	Agency administrative rules, agency financial rules, risk management policy	The organization has well functioning: <ul style="list-style-type: none"> <li>separation of duties</li> <li>asset registers</li> <li>physical security</li> <li>data security</li> <li>irregularity reporting</li> </ul>	
	The organization has an up-to-date contingency plan	Contingency plan	Updated and documented contingency plan	
Co-ordination of controls	Controls are integrated to the organization's management and steering processes	Planning guidelines, agency financial rules, process descriptions, policies and rules	Risk management is an integral part of planning and follow-up procedures	
	Controls of risks affecting several organizational units are coordinated	Risk management policy	Top management receives compiled risk reports and takes necessary action	
Follow-up of planned controls	Management monitors the efficiency of planned controls using risk and irregularity reporting	Risk management policy	Reports are produced systematically and they result in action	
	Effectiveness of controls are evaluated as part of risk analyzes	Risk management policy, assessment of internal control	Processes and controls attached to them are regularly evaluated and updated. Management evaluates irregularity reports.	
Follow-up of operations	Results are regularly compared with objectives and documented	Planning and follow-up documents, activity report	Planning, follow-up and reporting procedures include evaluation of realized results compared to objectives	
	Management takes action required by reported results	Planning process, Management meeting minutes	Management makes decisions based on follow-up reports. Decisions are carried out.	
	Results are communicated in a timely	Business unit meeting minutes, Intranet,	Personnel receives relevant information	

	manner to personnel and steering bodies	personnel satisfaction reports	about results and actions.	
	Risk information is used as an organizational learning tool.	The organization has capacity to engage employees in discussions of risks, deriving further insight and application in a practical way.	Debriefing sessions, learning forums.	

## Information and communication

Efficient information and communication systems will support interaction and reporting within the organization between management, employees and stakeholders.

SUB-AREA	ISSUE	REFERENCE	VERIFICATION	CONCLUSION
Management accounting	Management accounting in the organization fulfils requirements of policy or law.	Accounting framework and systems, HR systems, MIS, quality systems, customer reports, strategy and follow-up	The organization produces information required by budget act and budget decree for all areas of the performance prism. Information from different systems and methods can be combined to produce organization wide reporting. Management on all levels uses information from management information systems.	
Internal communication	The organization has adequate methods to support information and communication	Unit meetings, information channels, intranet, management group, co-operation meetings, employee satisfaction reports	Employees on different levels have adequate information to fulfil their tasks.	
	The organization has quick and clear communication methods for emergency situations	Communication plan, anomaly reporting, whistle blowing rules	Emergency communication plans exist and are communicated to personnel.	
	The organization has methods to communicate personnel and stakeholder views to management	Customer feedback systems, employee feedback systems	Employee satisfaction is regularly measured.	
Management information systems	The organization is capable of producing true and adequate information required by the budget act	Annual report, strategy follow-up	Information from MIS fulfils the needs for the performance prism and 55 § of the budget act	
External communication	The organization has quick and clear communication methods for emergency situations	Communication plan, contingency plan	An emergency situation communication plan exists	
	The organization has methods to communicate with stakeholders	Communication plan, co-operation groups, customer satisfaction reports	The organization uses agreed ways of communication with its stakeholders. Customer satisfaction is evaluated regularly.	
Third Party Risk Communication and problem Solving	Where the organization has a risk-dependency relationship with either third party providers or supply contractors, means are established to effectively communicate and mitigate risks on a continuing basis.	Mutual risk identification, definition and resolution about risks that each pose to the other or that they may share as a result of the contractual relationship.	Regular meetings. Sharing of information, formal understanding and problem-solving mechanisms.	

## Monitoring

SUB-AREA	ISSUE	REFERENCE	VERIFICATION	CONCLUSION
Continuous monitoring	Reporting on internal control is embedded to operational processes	Operational reporting, process evaluations, anomaly reports, customer feedback reports, self assessments, employee feedback reports	Operational reports are reconciled and evaluated regularly	
Internal evaluations	The organization evaluates annually the status of its internal control and gives an assessment in its annual report.	Annual report, budget act,	Status of internal control is regularly and systematically evaluated. Results from these evaluations lead to action. Annual assessment of the appropriateness and adequacy of internal control and of the risk management.	
	Internal audit reports are handled and decisions are made based on the reports	Internal audit policy, internal control framework	Internal audit reports are dealt with according to a systematic approach	
External evaluations	The organization evaluates annually reports from external auditors and makes necessary action plans	Management meeting minutes	Conclusions in external evaluations and audits are dealt with and lead to action.	
Governance Oversight	Governing bodies must have adequate information about the risk management profile and the management of it to assure itself that the organization is addressing these risks.	Governing bodies have a number of roles to play: <ul style="list-style-type: none"> <li>○ evaluating CEO performance,</li> <li>○ being informed of the understood risk profile</li> <li>○ providing guidance and input form a governance perspective</li> <li>○ assurance of follow-up and action.</li> </ul>	Linking risk to strategy in a formal way, possible specialized governance bodies responsible for risk management, board audit function, active review of risk information on a timely and appropriate level without interfering in the management of the organization.	