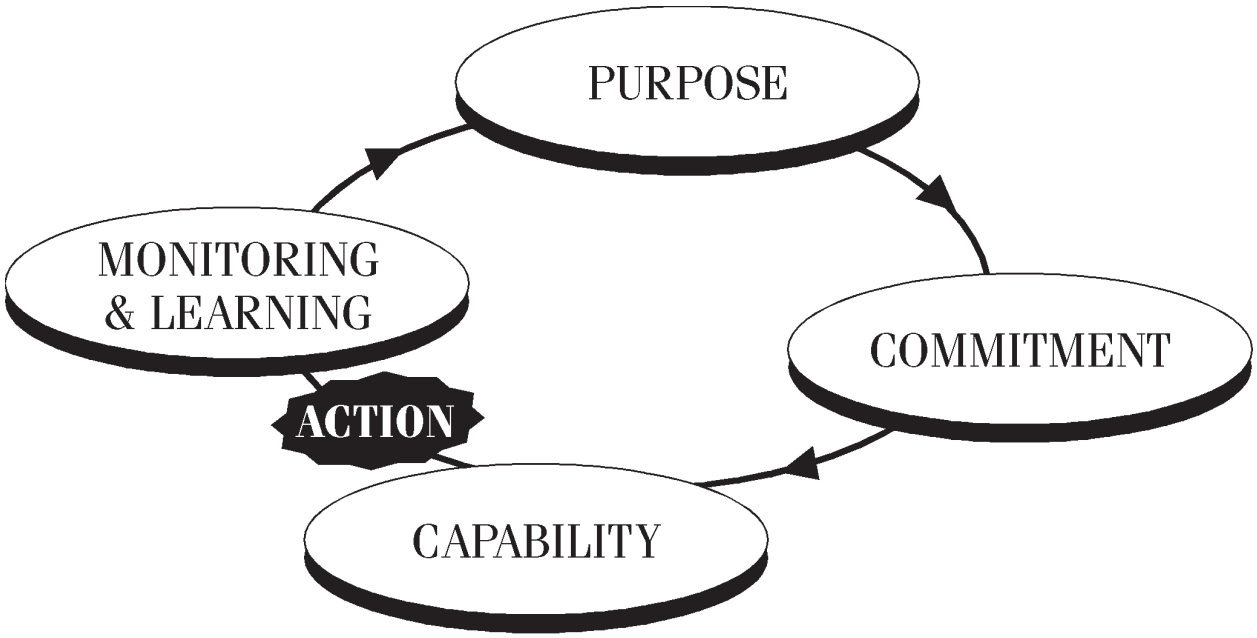
Guidance on Control



A person performs a task, guided by an understanding of its **purpose** (the objective to be achieved) and supported by **capability** (information, resources, supplies and skills). The person will need a sense of **commitment** to perform the task well over time. The person will **monitor** his or her performance and the external environment to **learn** about how to do the task better and about changes to be made. The same is true of any team or work group. In any organization of people, the essence of control is purpose, commitment, capability, and monitoring and learning.

Publications in the Control and Governance series

Preface to Guidance issued by the Criteria of Control Board (November 1995)
Guidance on Control (November 1995)
Guidance for Directors – Governance Processes for Control (December 1995)

Canadian Cataloguing in Publication Data

Canadian Institute of Chartered Accountants.
Criteria of Control Board
Guidance on control

ISBN 0-88800-436-1

1. Organizational effectiveness. 2. Management.
3. Systems analysis. I. Title.

HD58.9.C35 1995 658 C95-932623-5

The Canadian Institute of Chartered Accountants
277 Wellington Street West
Toronto, Ontario
M5V 3H2

Printed and Bound in Canada
Disponible en français

ISBN 0-88800-436-1

FOREWORD

The Criteria of Control Board of the CICA has written this guidance for people who are responsible for or concerned about control in organizations. They include:

- Boards of directors and other governing bodies
- Senior and line management
- Owners, investors and lenders
- Auditors

The term "control" in this guidance has a broader meaning than internal control over financial reporting. Terms defined in the glossary are printed in italics when first used.

The guidance is not a set of minimum requirements. Rather it offers a framework for making judgments about control. It includes a definition of control and twenty "criteria of control" which we describe, explain and discuss. Individual organizations will need to interpret and adapt the criteria to fit their own particular situations. In subsequent publications we shall provide more detailed guidance on the implications for governing bodies, control assessment and external reporting.

Many organizations use criteria similar to those set out in this guidance and their managements are well-placed to provide information on control to their governing bodies and owners. Others will need time to develop methods for assessing control, particularly in respect of criteria that deal with subjective attitudes and beliefs, and for assessing the significance of findings.

The guidance does not replace or extend the professional standards defined in the *CICA Handbook* for the scope of an external audit. It does, however, address conditions that can significantly affect the effectiveness of internal controls and the degree of audit risk.

We encourage:

- governing bodies and managers to use this guidance to help them improve the efficiency and effectiveness of their organizations and to demonstrate they have done so;
- owners, investors, lenders and others to use this guidance in making decisions about organizations in which they have an interest; and
- internal auditors and external auditors, within their mandate, to use this guidance to orient and conduct their work.

This guidance should be read in the context of the "Preface to Guidance issued by the Criteria of Control Board".

This guidance reflects evolving thinking on control. The Board expects to issue additional guidance as experience is gained. We encourage users of this guidance to describe their experience in using it and to provide suggestions for its further development by writing to the Director, Criteria of Control, The Canadian Institute of Chartered Accountants, 277 Wellington Street West, Toronto, Ontario M5V 3H2.

TABLE OF CONTENTS

INTRODUCTION

1 This guidance is intended to help improve *control*.[1] It describes and defines control (going well beyond a discussion of traditional internal accounting controls) and sets out criteria for *effective control* in an *organization*. It provides a *framework* that people throughout an organization can use to develop, assess and change control.[2] It does not, however, provide detailed guidance on how to design an organization – there are many methodologies described in management textbooks.

2 Effective control supports the success of an organization in several ways:

- People can exercise their judgment and creativity, while managing the risk of inappropriate actions.
- People have the flexibility to address change while addressing known risks.
- People have reliable information and are able to make use of it at the right time and at the most appropriate place in the organization.
- The organization can achieve improved effectiveness and efficiency, and greater confidence on the part of external parties.

THE NATURE OF CONTROL

3 An organization may be defined in various ways. In this guidance, an organization is understood to be people working in pursuit of *objectives*. Thus the objective becomes the defining factor of what is included or excluded from the organization.

4 Accordingly, an organization may be a legal entity such as a company, partnership or government agency, or sub-units of a larger organization such as divisions or departments. An organization may also be the entire system or process that produces the outputs to meet a particular objective. Such a system or process may cut across the formal organizational structure.

---

[1] Terms included in the Glossary of Terms (Exhibit A) are printed in italics when first used.

[2] This guidance builds on the understanding of control found in the U.S. publication "Internal Control – Integrated Framework" (Committee of Sponsoring Organizations of the Treadway Commission, New Jersey, 1992). It is the belief of the Criteria of Control Board that organizations that follow this guidance will have thereby considered the components of the COSO framework. Appendix 1 provides a comparison of the control framework outlined in this guidance with the framework provided by COSO.

5 The smallest unit of an organization is the individual person. A person performs a task, guided by an understanding of its **purpose** (the objective to be achieved) and supported by **capability** (information, resources, supplies and skills). The person will need a sense of **commitment** to perform the task well over time. The person will **monitor** his or her performance and the external environment to **learn** about how to do the task better and about changes to be made. The same is true of any team or work group. In any organization of people, the essence of control is purpose, commitment, capability, and monitoring and learning.

6 Control comprises those *elements* of an organization (including its resources, systems, processes, culture, structure and tasks) that, taken together, support people in the achievement of the organization's objectives. These objectives may fall into one or more of the following general categories.

- **Effectiveness and efficiency of operations** includes objectives related to an organization's goals, such as customer service, the safeguarding and efficient use of resources, profitability and meeting social obligations. This includes the safeguarding of the organization's resources from inappropriate use or loss and ensuring that liabilities are identified and managed.

- **Reliability of internal and external reporting** includes objectives related to matters such as the maintenance of proper accounting records, the reliability of information used within the organization and of information published for third parties. This includes the protection of records against two main types of fraud: the concealment of theft and the distortion of results.

- **Compliance with applicable laws and regulations and internal policies** includes objectives related to ensuring that the organization's affairs are conducted in accordance with legal and regulatory obligations and internal policies.[3]

7 Control is effective to the extent that it provides reasonable assurance that the organization will achieve its objectives reliably. Or, stated another way, control is effective to the extent that the remaining (uncontrolled) risks of the organization failing to achieve its objectives are deemed acceptable. Control therefore includes the identification and mitigation of risks. These risks include not only known risks related to the achievement of a specific objective but also two more fundamental risks to the viability and success of the organization:

- failure to maintain the organization's capacity to identify and exploit opportunities; and

- failure to maintain the organization's resilience. Resilience refers to the organization's capacity to respond and adapt to unexpected risks and opportunities, and to make decisions on the basis of telltale indications in the absence of definitive information.

[3] The board of directors may discharge part of its responsibility for monitoring control through committees. For example, the audit committee usually oversees accounting and financial reporting. Monitoring other aspects of control may be performed by the audit committee, by other committees or by the whole board.

8 The following concepts are important in understanding the nature of control.

(a) **Control is effected by people throughout the organization, including the board of directors (or its equivalent)[4], management and all other staff.**

People are responsible for designing, implementing, monitoring and maintaining control. It follows that control is affected by the many organizational influences on people's motivations and behaviour.

(b) **People who are accountable, as individuals or teams, for achieving objectives should also be accountable for the effectiveness of control that supports achievement of those objectives.**

It follows that people (whether they have the title of manager or not) are responsible for assessing the effectiveness of control in the tasks, team or unit for which they are accountable, and for communicating such assessments to those to whom they are accountable.

(c) **Organizations are constantly interacting and adapting.**

Organizations are constantly adapting in response to changes in the *external environment* (e.g., in customers, suppliers and regulation) and changes in the *internal environment* (e.g., in people and priorities). For control to be effective, the control elements in an organization must fit with its objective, be consistent with each other, and change and adapt. This means that when changes are contemplated to any aspect of an organization, the control consequences should be considered.

(d) **Control can be expected to provide only reasonable assurance, not absolute assurance.**

There are two basic reasons why absolute assurance is not possible, even though due care and diligence may have been exercised.

First, there are inherent limitations in control. These include the possibility of faulty judgment in decision-making, of breakdowns because of human error, of control activities being circumvented by collusion of two or more people and of management overriding control. Control can help minimize the occurrence of errors and breakdowns but cannot provide absolute assurance that they will not occur.

Second, cost/benefit considerations can and should be taken into account when designing control in organizations. The costs of control must be balanced against the benefits, including the risks it is designed to manage. Design decisions involve the acceptance of some degree of risk: outcomes or actions cannot be predicted with absolute assurance.

[4] The governing body of a government or not-for-profit entity may be called by a different name. In a unit within an organization, the equivalent to the board of directors is the senior management or other leadership group.

Exhibit A
GLOSSARY OF TERMS

Control	Control comprises those elements of an organization (including its resources, systems, processes, culture, structure and tasks) that, taken together, support people in the achievement of the organization's objectives.
Control activities	Routines established to provide assurance that processes operate as designed and meet the requirements of the organization's policies.
Control element	Any part of an organization, or the relationship between parts of an organization, that contributes to reliable achievement of its objectives.
Control framework	A way of understanding the important elements of control including the important relationships between them. In this guidance, the control framework consists of the definition of control, the criteria of control and how the criteria are grouped.
Criteria of control	The 20 criteria numbered A1 to D6. Criteria of control are the basis for understanding control in an organization and for making judgments about the effectiveness of control.
Effective control	Control is what makes an organization reliable in achieving its objectives. Control is effective to the extent that it provides reasonable assurance that the organization will achieve its objectives. Or, stated another way, control is effective to the extent that the remaining risks of the organization failing to meet its objectives are deemed acceptable.
External environment	Includes those factors external to an organization that influence or affect it (for example, customers, suppliers, competitors, the economy, laws, regulators and social conditions).
Internal environment	Includes those factors internal to an organization that influence or affect it including all aspects of control and all the systems and processes of the organization.
Objectives	The goals that an organization sets for itself. At an overall level they may be general statements, while at more detailed levels they may be specific.
Organization	People working in pursuit of objectives. The entity as defined from time to time, including its governing body (e.g., board of directors). An organization may be an incorporated or unincorporated company, a sole proprietorship, a partnership, a government or a not-for-profit enterprise. It may also be a sub-unit of a larger organization (e.g., a division, department or process).

(e) **Effective control demands that a balance be maintained:**

(i) Between autonomy and integration.

Keeping this balance often involves shifting between centralization and decentralization, and between imposing constraints to achieve consistency and granting freedom to act.

(ii) Between the status quo and adapting to change.

Keeping this balance often involves shifting between demanding greater consistency to gain efficiency and granting greater flexibility to respond to change.

THE DISTINCTION BETWEEN CONTROL AND MANAGING

9 An assessment of control is necessarily an assessment, albeit partial, of how the organization is managed. Nevertheless, control does not constitute everything involved in managing an organization. Control supports the reliable achievement of objectives: it does not tell people what objectives to set. Control can help ensure that the people responsible for monitoring and decision-making have appropriate, reliable information. It can follow and report on the results of actions taken, or of decisions not to act; and the information provided may lead to further management decisions or actions. Control cannot, however, prevent the taking of strategic and operational decisions that are, in retrospect, incorrect. Decisions about whether to act and what action to take are aspects of managing that are outside of control.

APPLICABILITY

10 This guidance is intended to be useful primarily to directors, managers and other people who are accountable for control in an organization or part of an organization. It is also intended to be useful as a basis for people to assess the effectiveness of control in an organization.

11 This guidance is applicable to all kinds of organizations, including profit-oriented enterprises in the private and public sectors, not-for-profit organizations, governments and government agencies. It is applicable equally to a whole organization, to a part of an organization (such as a division, group, team or individual), and to a business process (such as the delivery of a service).

12 This guidance is applicable also to various management approaches. These approaches cover a broad spectrum including the "top-down, command-and-control" approach characterized by a concentration of authority in the hands of senior ranks, and the "empowered" approach characterized by reduced layers of management, with discretionary authority placed close to the front line. Management approaches closer to the former end of the spectrum tend to place greater emphasis on formal control features, such as detailed policies and approvals. Those closer to the latter end typically place greater emphasis on informal features, such as shared vision and values, based on two key assumptions about how people function within systems:

(a) people will cooperate toward the achievement of the organization's objectives to the extent that the organization supports such cooperation, for example through open communications and human resource policies and reward systems; and

(b) people have the capacity and willingness to exercise control over the activities in which they are engaged.

13 This guidance provides for flexibility in how control is implemented. It does not prescribe a set of detailed policies and procedures.

14 Different organizations will place greater or lesser emphasis on each criterion in this guidance. For example, small organizations typically need fewer formal mechanisms to achieve control than do large organizations, because communication is more direct. Volunteer organizations often place relatively more reliance on the shared values that motivate volunteers, and less on routine control activities (although these still have their place). Within a single organization, the emphasis may differ from department to department and change over time.

PARTICIPANTS IN CONTROL

15 People throughout an organization participate in and have responsibility for control. That responsibility does not belong exclusively to the controller or internal auditor. Through their decisions and actions, the board of directors (or its equivalent) and senior management set the tone that influences the direction of decisions and actions throughout the organization.

16 The board of directors (or its equivalent) is responsible for the stewardship of the organization, including the following control responsibilities.

- Approving and monitoring mission, vision and strategy
- Approving and monitoring the organization's ethical values
- Monitoring management control
- Evaluating senior management
- Overseeing external communications
- Assessing the board's effectiveness

These responsibilities are discussed in the publication "Guidance for Directors – Governance Processes for Control".

17 The responsibility for control exists throughout the organization in conjunction with accountability for achieving objectives. This responsibility may be explicit, but it may not be, especially where control is not thought of as separate from accountability for performance. For example, a plant manager may have production and efficiency objectives. Effective control will help the plant manager ensure that the objectives are achieved, but the control responsibility may not be explicitly stated because it is deemed to be implicit.

18 Management participates in control and is also accountable for it, and therefore needs to assess its overall functioning. Depending on the size and nature of the organization, management may choose to conduct the assessment itself, or to rely on a specific function within the organization or an independent third party to perform some of the work.

CONTROL FRAMEWORKS

19 A control framework provides a way of understanding the important elements of control, including the important relationships between them. In this guidance, the control framework consists of the definition of control, the *criteria of control* and the grouping of criteria. The criteria and their grouping are shown in Exhibit B.

20 The control framework in this guidance provides a useful, comprehensive way of looking at control. This guidance needs to be creatively interpreted and applied. An organization may adopt the framework set out here or use it to develop or modify its own.

21 Any grouping of the criteria highlights some aspects of control more than others. Criteria can be grouped to suit particular circumstances, but all the criteria need to be considered in the regrouping.

22 For example, an organization may have adopted a management approach that has its own routines and vocabulary. Applying the control framework in this guidance does not mean that these must be discarded. Instead, the current management approach can be compared to the control framework and modified as necessary to address control. Included in Appendix 1 is a regrouping of these criteria into the structure used in "Internal Control – Integrated Framework" (Committee of Sponsoring Organizations of the Treadway Commission, New Jersey, 1992). Appendix 2 shows how a total quality management model may be compared to the control framework in this guidance.

THE CRITERIA

23 The criteria of control are the basis for understanding control in an organization and for making judgments about the effectiveness of control. The criteria are formulated to be broadly applicable. The effectiveness of control in any organization, regardless of the objective it serves, can be assessed using these criteria.

24 The criteria of control are set out in Exhibit B, and supporting explanation is provided in the following pages. The criteria are phrased as goals to be worked toward over time; they are not minimum requirements to be passed or failed. Considerable judgment is required in interpreting the criteria in the context of a particular organization and in assessing the effectiveness of control in the organization.

25 Criteria need to be interpreted in the context of particular objectives. For a customer-service objective, the criterion that deals with monitoring performance might be interpreted in terms of order-filling accuracy and promptness, and customer feedback. For an employee-morale objective, the same criterion might be interpreted in terms of absentee levels and morale surveys. All of the criteria are relevant to every organization, though some may be more important than others in any particular case.

26 The effectiveness of control cannot be judged solely on the degree to which each criterion, taken separately, is met. The criteria are interrelated, as are the control elements in an organization. Control elements cannot be designed or evaluated in isolation from each other.

27 The same criteria, and the same control framework, can be applied to an entire organization and to discrete parts of an organization. For example, monitoring can be considered for the organization as a whole or for a particular division, department, business process, work group or team or even for an individual. Similarly, risks can be identified for the organization as a whole and for an individual operating unit.

Exhibit B
THE CRITERIA

Purpose

A1 Objectives should be established and communicated.

A2 The significant internal and external risks faced by an organization in the achievement of its objectives should be identified and assessed.

A3 Policies designed to support the achievement of an organization's objectives and the management of its risks should be established, communicated and practised so that people understand what is expected of them and the scope of their freedom to act.

A4 Plans to guide efforts in achieving the organization's objectives should be established and communicated.

A5 Objectives and related plans should include measurable performance targets and indicators.

Commitment

B1 Shared ethical values, including integrity, should be established, communicated and practised throughout the organization.

B2 Human resource policies and practices should be consistent with an organization's ethical values and with the achievement of its objectives.

B3 Authority, responsibility and accountability should be clearly defined and consistent with an organization's objectives so that decisions and actions are taken by the appropriate people.

B4 An atmosphere of mutual trust should be fostered to support the flow of information between people and their effective performance toward achieving the organization's objectives.

Capability

C1 People should have the necessary knowledge, skills and tools to support the achievement of the organization's objectives.

C2 Communication processes should support the organization's values and the achievement of its objectives.

C3 Sufficient and relevant information should be identified and communicated in a timely manner to enable people to perform their assigned responsibilities.

C4 The decisions and actions of different parts of the organization should be coordinated.

C5 Control activities should be designed as an integral part of the organization, taking into consideration its objectives, the risks to their achievement, and the inter-relatedness of control elements.

Monitoring and Learning

D1 External and internal environments should be monitored to obtain information that may signal a need to re- evaluate the organization's objectives or control.

D2 Performance should be monitored against the targets and indicators identified in the organization's objectives and plans.

D3 The assumptions behind an organization's objectives should be periodically challenged.

D4 Information needs and related information systems should be reassessed as objectives change or as reporting deficiencies are identified.

D5 Follow-up procedures should be established and performed to ensure appropriate change or action occurs.

D6 Management should periodically assess the effectiveness of control in its organization and communicate the results to those to whom it is accountable.

PURPOSE

Purpose groups criteria that provide a sense of the organization's direction. They address:

- objectives (including mission, vision and strategy)
- risks (and opportunities)
- policies
- planning
- performance targets and indicators

A1 Objectives should be established and communicated.

28 Objectives provide direction. They may relate to the organization as a whole or to parts of it, and they may have different degrees of detail. Objectives may be long-term or short-term in nature, and they may be classified in one or more general categories: effectiveness and efficiency of operations, reliability of internal and external reporting, and compliance with applicable laws and regulations and internal policies.

Mission, vision and strategy

29 The mission and vision represent the organization's overall objectives. The mission is the organization's reason for existing. It may be inherited from the founders or from others, or it may be renewed in response to changing circumstances. In a government organization, the mission may be stated in or inferred from the legislation that created it or the program under which it operates. The vision is the future state to which the organization aspires. As used here, it includes the organization's strategic objectives and the plans to realize them.

30 An explicit mission and clear vision, shared throughout the organization, can hold it together and on course, providing cohesion during change. They are thus key elements of control and should be approved by the board of directors, or its equivalent. The mission and vision will be more effective control elements if people have a personal stake in them.

More detailed objectives

31 More detailed objectives express the mission and vision in specific terms relevant to the organization or parts of it. People need to understand their role in achieving the overall objectives. They are then in a position to set and communicate local objectives aligned with them.

32 Sometimes the "cascading" of objectives from the overall level to the local level will follow the organization's hierarchy. For example, the chief financial officer will hold the controller responsible for the integrity of financial information to support decision-making; the controller will hold the accounts receivable group responsible for the accurate recording of invoices and receipts to customer accounts, and so on. In other cases, the cascading will follow supplier/customer relationships between teams, departments or work units. Sometimes a local unit will need information or supporting action from more senior levels of the organization in order to achieve its objectives. Then, the "cascade" flows upwards in the hierarchy, in that local objectives drive the objectives and actions of more senior levels.

33 Operating units in the organization may receive central direction but still need to consider the local environment in setting objectives. For example, local management of a factory may receive direction from senior management yet must still consider the requirements and needs of parties such as the local bargaining unit and the municipal authorities.

Objective-setting

34 Deciding what objectives to adopt is, like other decision-making, an aspect of managing that is outside of control. The process of objective-setting, on the other hand, is within the definition of control.

35 Objective-setting involves identifying requirements that must be met, and identifying and balancing risks and opportunities associated with those requirements, and the needs and wants of various parties (both internal and external). Objective-setting thus requires an understanding of the organization's mission and vision, the environment in which it operates and its position within that environment. Objective-setting is a continuing process, requiring monitoring of operating performance and of changes in the internal and external environments.

36 Balancing different needs is necessary because every organization affects various parties who in turn desire to influence it. It is up to the people in charge to decide the extent to which they will try to meet these desires. For example, when management develops strategic objectives, and when the board of directors reviews them, they may need to consider the interests of lenders, employees, customers and others, as well as the interests of shareholders and legal and regulatory requirements.

37 Objective-setting can be formal or informal, depending on factors such as the size, structure and needs of the organization. Objectives for the entire organization may be represented through formal or informal statements, but should be specific enough to provide effective direction for risk assessment and planning. These objectives also need to be clearly communicated so that people understand the context and direction for their decisions, actions and coordination.

Conflicting objectives

38 Organizational objectives may often appear to be in conflict. For example, a bank may simultaneously seek growth in its loan portfolio and maintenance of loan quality. Some organizations seek to redefine objectives to eliminate conflict, or segregate functions so that no individual or group is placed in a double bind. Other organizations view conflicting objectives as inevitable and treat them as a desirable source of creative tension to be openly addressed.

39 In either case, the organization should have a process to address situations where objectives come into conflict. This process can provide a resolution for the immediate situation, and examine deeper considerations, such as whether apparent conflicts are actually in opposition, whether they represent differences in priorities, and whether they are desirable or undesirable manifestations of internal competition.

A2 The significant internal and external risks faced by an organization in the achievement of its objectives should be identified and assessed.

40 Any course of action or inaction involves some risk to the achievement of objectives. Risks are acceptable if their avoidance is not cost-justified. This would be the case where the cost of preventive measures would outweigh the risk avoided, or where risks inevitably accompany opportunities that the organization cannot afford to ignore. Risks and opportunities are closely related. For example, a failure to identify a significant opportunity may become a risk if it results in existing objectives not being met or in existing objectives not being changed.

Scope

41 An organization needs to identify its significant internal and external risks on an ongoing basis so that it can react to (or initiate) changes in an appropriate and timely manner. Risk identification should extend to all objectives, including those that are not explicitly stated. For example, the objective of staying in operation may not be stated, but it may be affected by the risks that stem from noncompliance with laws. While it is rarely cost-beneficial to try to identify all risks, such identification needs to be comprehensive enough to provide reasonable assurance that those risks which may significantly affect objectives have been identified.

42 Risk assessment involves estimating the likelihood of an event and the significance of its consequences so that appropriate policies and processes can be developed to manage them. The risks of failure can rarely if ever be reduced to zero (even if that were desirable from a cost-benefit point of view).

43 Accordingly, people need to know what risks are acceptable to senior management and the board of directors. In turn, senior management and the board need to understand what risks are acceptable to the organization's other stakeholders. Explicit recognition of the residual risks that have been accepted and communication of that recognition throughout the organization is essential for effective control.

44 Risk identification and assessment should be performed for each significant objective of the organization. Centralized risk identification and assessment across functions usually needs to be combined with local risk assessment to provide a useful overview.

Sources of risk

45 Risk identification and assessment starts with an understanding of the environments, both internal and external, that influence risk. Risk stems from the environments in which the organization operates (for example, the markets it chooses, the technology it selects, competitors' strategies and customers' perceptions) and from the way it participates in and influences those environments (for example, the extent to which it uses lobbying, advertising and marketing techniques to shape those markets).

46 Risk also stems from choices made about how the organization will function. For example, operating systems that are highly centralized, complex and tightly integrated may carry significant risks; diverse, decentralized systems will carry different risks. Certain risks, such as people making mistakes or misappropriating resources, are found in most organizations.

A3 Policies designed to support the achievement of an organization's objectives and the management of its risks should be established, communicated and practised so that people understand what is expected of them and the scope of their freedom to act.

47 Policies prescribe how things should be done and prohibit inappropriate action, thus providing the limits of acceptable action. If people are to exercise their judgment and creativity in the interests of the organization, they must understand these limits and be free to act within them. Policies need occasional reviews to guard against them growing too detailed or irrelevant.

48 Understandable policies, communicated throughout the organization and translated into specific practices, provide direction on how operations are to be conducted and reflect a judgment as to which risks are deemed acceptable. Policies, together with objectives, provide the frame of reference for the design of control activities (discussed under C5 below).

49 Policies may be developed in a number of areas, such as customer relations, service levels, environmental protection, risk management, accounting and financial reporting, security, confidentiality and expenditures. The need for specific policies, and the extent to which they are documented, depend on the size of the organization, the objectives to be achieved, the risks involved and the extent to which clear communication of the limits of acceptable action is required.

A4 Plans to guide efforts in achieving the organization's objectives should be established and communicated.

50 Planning translates objectives and risk assessments into strategies, action plans and operating and financial targets against which progress can be measured and monitored. Planning is a continuing process, and plans should not be static. They may need to be changed if performance measurements indicate that the desired results are not achievable. They may also change if objectives, risks or other operating considerations change.

51 Planning includes the allocation of financial, physical and human resources. Resource allocation begins with the determination of what the organization needs to attain its objectives. Since resources are usually limited, their allocation also involves decisions on how they should best be distributed.

52 The adequacy of resources depends above all on their relationship to the objectives to be achieved and the risks to be assumed. For example, a reduction in budget to meet a financial objective is often associated with an increased risk of failing to meet other objectives, such as service levels.

53 The organization may need to be highly reliable so that it can continue to meet objectives even in the face of emergencies, breakdowns and periods of peak activity. In such cases, the organization can consider a range of control elements, depending on their relative costs and benefits. These might include maintaining a backup site for critical computer applications; using multiple messages to minimize communication errors; cross-training people so that they can assume each other's duties; keeping additional human and physical resources on standby; and establishing alternative sources of command to increase the organization's speed of response, ability to detect threats and opportunities, and creative decision-making. Different types of training may also be considered. For example, disaster simulations may play a key role in training for effective crisis management.

54 The formality of the planning process, the plans produced and their level of detail will depend on factors such as the size of the organization, its decision-making structure, and the necessity of giving or receiving formal approval for certain activities. The effective communication of plans is integral to the organization's ability to direct people's efforts to achieve its objectives. Where plans are also prepared at the local level, they should be consistent with the overall plan.

A5 Objectives and related plans should include measurable performance targets and indicators.

55 Organizations may use a mixture of quantitative performance targets, such as budgets, and qualitative performance targets, such as customer satisfaction. These targets should be measurable and aligned with the objectives. Externally derived benchmarks can be used to help ensure such targets are competitive.

56 Performance indicators can be used to measure performance against targets and to provide early warning if targets have been exceeded or have not been met. Where qualitative performance targets are used, the related indicators need to be expressed in such a way that they can be applied objectively and reasonably. For example, customer satisfaction could be measured by examining customer complaints or returns.

COMMITMENT

Commitment groups criteria that provide a sense of the organization's identity and values. They address:

- ethical values, including integrity
- human resource policies
- authority, responsibility and accountability
- mutual trust

B1 Shared ethical values, including integrity, should be established, communicated and practised throughout the organization.

57 All control rests ultimately on people assuming responsibility for their decisions and actions. Organizational values that people find acceptable encourage them to assume responsibility for the continuous improvement of their organization.

58 Personal values may differ widely because of diversity in people's backgrounds and experience. For organizational values to be shared, it is important that the process of developing and maintaining them respect this diversity.

59 Shared ethical values influence all behaviour in an organization. Together with an understanding of mission and vision, they constitute the basic identity that will shape the way an individual, group, organization or board will operate, and they provide stability over time. Shared values contribute to control because they provide a guide for individual, group or team decision-making, action and policy.

60 The values and preferences of senior management and the board of directors greatly influence an organization's objectives and systems. These values and preferences address issues such as:

- good corporate citizenship;
- commitment to truth and fair dealing;
- commitment to quality and competence;
- leadership by example;
- compliance with laws, regulations, rules and organizational policy;
- respect for the privacy of client, organization and employee information;
- fair treatment of and respect for individuals;
- fair relationships with competitors;
- integrity of transactions and records; and
- a professional approach to financial reporting.

61 An organization's values find expression in almost every aspect of its existence. If the values lived out in the organization differ from those set out in approved policies, people will ignore the policies. That is why expectations concerning behaviour must be clearly communicated and understood throughout the organization and supported by the actions of management and the board. Management also needs to monitor actual behaviour against such expectations and deal appropriately with any deviations.

62 To act in accordance with an organization's values, people need support and open communication – especially when it comes to helping them deal with dilemmas and uncertainty relating to ethical conduct. People need to feel free to communicate their concerns regarding ethical issues without fear of repercussion. Management needs to create a supportive environment for this communication to occur.

63 Ethical values are part of an organization's culture and provide an unwritten code of conduct against which behaviour is measured. A formal, written code of conduct offers a means for consistent communication of the standards of ethical behaviour. People can be asked periodically to confirm their understanding and observance of the code.

B2 Human resource policies and practices should be consistent with an organization's ethical values and with the achievement of its objectives.

64 While A3 is applicable to all policies, human resource policies and practices are highlighted here because of their significance. Control is effected through people; their behaviour and motivation are affected by human resource policies, practices and reward systems.

65 Human resource policies and practices may address matters such as performance evaluation, promotion, compensation, remedial action, training, termination, recruitment, career development, health and safety, equity, harassment and discrimination. Management's response to noncompliance with these policies should support the organization's ethical values.

66 People's behaviour is influenced by how they believe themselves to be managed and rewarded. Accordingly, reward systems and performance measures should be consistent with the organization's ethical values, support the achievement of its objectives, and be clearly communicated. A pattern of error or dysfunctional behaviour, such as extremes in risk-taking or risk aversion, may indicate an inappropriate reward system.

67 Reward systems include financial and non-financial incentives and sanctions. Some rewards can be given by the organization, such as increased responsibilities, greater autonomy, public recognition for achievement and financial payment. Other rewards stem from individual motivation and might include pride in achievement, peer recognition and a sense of meaningful contribution.

68 Performance measures may be explicit, as in formal appraisal methods, or implicit, as in the measures thought to have been applied in awarding promotions. Performance measures need to be carefully developed if objectives such as the following are to be achieved: consistency in rewards, balance of short- and long-term factors, avoidance of blaming individuals for problems attributable to the organization, and offering rewards to the right work unit (individual or group).

B3 Authority, responsibility and accountability should be clearly defined and consistent with an organization's objectives so that decisions and actions are taken by the appropriate people.

69 Authority is the power to make certain decisions and/or perform certain tasks within defined limits. Responsibility is the duty to perform certain tasks. Accountability is the obligation to answer for the performance of responsibilities. An individual or group must be provided with the authority and responsibility for a task, output or outcome in order to be held accountable.

70 The extent to which people recognize that they will be held accountable influences their decisions and actions. That is why authority, responsibility and accountability should be clearly defined and communicated through (for example) task or job descriptions. The organizational structure will reflect and support this authority, responsibility and accountability.

71 Clearly defined authority, responsibility and accountability help ensure that critical decisions are made by qualified individuals. They help create the expectation that if an individual does not feel able to solve a problem, he or she will find someone with the necessary knowledge, expertise and authority to effect coordination with others. This migration of decision-making may be formally documented in the organization's authorization policies (for example, a bank may have a policy for certain loan decisions to be made by certain officers), or it may be established informally through commonly acknowledged norms of behaviour and shared values.

B4 An atmosphere of mutual trust should be fostered to support the flow of information between people and their effective performance toward achieving the organization's objectives.

72 Some level of mutual trust between people is essential to control. Mutual trust supports the flow of information that people need in order to make decisions and take action. It also supports the cooperation and delegation that are required for effective performance toward the achievement of the organization's objectives. Trust is based on confidence in the other person's or group's integrity and competence.

73 Open communication both creates and depends on trust within the organization. A high level of trust encourages people to ensure that everything of importance is known to more than one person. Sharing such information strengthens control by reducing the dependence on one person's continued presence, judgment and ability.

74 For example, people faced with difficult financial or operating problems may feel great pressure to withhold or cover up information in order to buy time. If they can trust the organization to distinguish innocent mistakes from blatant abuse or incompetence – and to treat such mistakes as a source of learning rather than as a basis of punishment – they are more likely to communicate problems and bad news quickly to others. In this way, trust permits frustrations, tension and breakdowns to serve the organization's achievement of objectives, rather than impede it.

75 The openness of communications and people's willingness to delegate are indications of the level of trust that exists. Changes in the organization, such as restructuring or downsizing, can affect an established atmosphere of trust, particularly if implemented in a manner inconsistent with the organization's values.

CAPABILITY

Capability groups criteria that provide a sense of the organization's competence. They address:

- knowledge, skills and tools
- communication processes
- information
- coordination
- control activities

C1 People should have the necessary knowledge, skills and tools to support the achievement of the organization's objectives.

76 The right match of people and tasks to be performed helps ensure that people are capable of performing the tasks necessary to support the achievement of the organization's objectives.

77 Having people with the necessary skills and capabilities starts with personnel selection. Human resource policies and practices in this area might include defining required competencies, using employment criteria, and performing background checks on candidates.

78 Ongoing assessment of requirements and resources results in decisions concerning training, supervision, task assignment and redeployment. It may also result in the use of outside services to meet requirements that cannot be met by the organization's employees.

79 Training may focus on skills to support individual performance and interpersonal skills necessary to support group decision-making and learning. Both the individual and the organization have an interest in the development of competence, although the degree of responsibility assumed by each differs from organization to organization.

80 Tools include machinery and equipment as well as software, patents and work methodologies and other 'soft assets'. Inadequate tools or improper training in their use can be a cause of inefficiency and ineffective control.

C2 Communication processes should support the organization's values and the achievement of its objectives.

81 For control to be effective, an organization needs to have communication processes capable of supporting two-way, open communication of timely, relevant and reliable information.

82 Communication processes serve a number of purposes. Different processes may be needed for transmitting commands, reaching agreement on resource allocations, coordinating activities, seeking information and for urgent communication about risks and opportunities. These processes may be formal (as in periodic meetings and reports) or informal (as in ad hoc discussions on newly identified concerns), and they may be used at regular or irregular intervals. Anonymous processes should be available for reporting problems or sensitive issues.

83 Communication processes are used to convey a wide variety of matters, including expectations about ethical values; policies; authority, responsibility and accountability; the objectives of the organization and plans to achieve them. Many other examples are cited throughout this guidance. Communication processes need to convey feedback about operating performance and about the environment within and outside the organization, as discussed in Section D – Monitoring and Learning.

84 Two-way communication helps to ensure that communication processes are flexible and responsive, both within the organization and between it and the external parties that are important to its activities. Obtaining the views of those most directly affected by a decision is often key to the subsequent success of implementation. Communication processes need to accommodate people's different capacities to handle data and communication responsibilities. Too much data can be as harmful as too little.

C3 Sufficient and relevant information should be identified and communicated in a timely manner to enable people to perform their assigned responsibilities.

85 People need an open flow of timely information from inside and outside the organization. For example, a group needs to know promptly about changes in customer requirements in order to quickly change its processes – or its customers – to adapt to the threat or opportunity. Similarly, people should provide information to others. For example, if a group responsible for a manufacturing process receives poor supplies, it must inform its suppliers; if it receives negative reports from its customers, it must inform its own people, suppliers, or both.

86 Risk is mitigated when people making decisions have the relevant information to see the big picture. They need to be able to integrate quantitative information, such as performance reports and indicators of change, with qualitative information, such as employee attitudes and rumours of supplier or labour unrest. Information should flow to decision-makers from various areas inside and outside the organization to enable them to identify emerging patterns that signal a risky or hazardous situation in its infancy.

87 For monitoring to be effective, the information gathered needs to be relevant and reliable, accessible by or directed to those who have the authority to act on it, and collected quickly enough for effective decision-making. Information is relevant to a user to the extent that it deals with matters within the user's responsibility and to the extent that the user is able to appreciate its significance. Cost/benefit trade-offs will be made in determining the information to collect and how it is collected and distributed.

88 Monitoring occurs through formal and informal communication processes. The organization's culture will affect the amount, type and reliability of information available through these processes. For example, an organization with a structure that includes cross-functional teamwork may be able to get significant amounts of reliable information from informal processes while a more hierarchical organization may rely primarily on formal reports, supplemented by informal processes.

C4 The decisions and actions of different parts of the organization should be coordinated.

89 Most individuals interact with other people as part of a group. The board of directors can be thought of as a group, as can a night-shift production unit or a task force assembled to address a special project. The organization as a whole can be thought of as a group composed of sub-groups, composed of sub-sub-groups ... composed of individuals. They are all suppliers or customers of some kind, whether of information, physical goods, or other resources.

90 Accordingly, decisions and actions almost always require coordination. For control in an organization to be effective, it is not enough for sub-groups to achieve their local objectives: they must also work together as a whole organization.

91 Coordination improves integration, consistency and accountability, and limits autonomy. Frequently, sub-groups must sacrifice some degree of effectiveness in achieving local objectives in order to enhance the effectiveness of the organization as a whole. For example, a manufacturing operation might have as an objective the minimization of unit production costs. Nevertheless, it might refrain from achieving such minimization through economies of scale if the resulting volume would overwhelm inventory and distribution capacity.

92 It is therefore essential that people consider the consequences of their decisions and actions for the organization as a whole. This will usually entail advance consultation within and between organizational units. Problems are particularly likely to occur when a system spans two or more departments, because people in one may be unaware of what people in the other do.

93 Complex organizations may demand a more formal control activity to achieve coordination. This may be effected either through an individual, such as a unit manager, or an activity, such as regular production control meetings.

C5 Control activities should be designed as an integral part of the organization, taking into consideration its objectives, the risks to their achievement, and the inter-relatedness of control elements.

Design and integration

94 *Control activities* are routines established to provide assurance that processes operate as designed and meet the requirements of the organization's policies. Everyone in the organization is likely to have some responsibility for control activities.

95 Some control activities are integrated with computer systems, such as an edit check in a computer program. They would be performed even if no assurance of reliable performance were needed. Designing control activities into computer systems is preferable to adding them afterward because no incremental costs are incurred.

96 Other control activities may be performed solely to increase the assurance of reliable performance, such as measures for safeguarding assets through safes, alarm systems, passwords and so on. These activities usually cost time and money, and restrict people's autonomy. The decision to add control activities should take into account costs, benefits, and what residual risks are acceptable.

97 Other considerations in the design and selection of control activities include the policies of the organization, the nature of its products and services, the importance of consistent treatment of customers, the organization's size and structure, and the complexity of its information systems. Control activities may also be designed to achieve such goals as balancing the prevention of errors and their detection, having activities occur on a timely basis, and segregating incompatible functions as far as possible.

98 Examples of common control activities include observing, comparing, approving, reporting, coordinating, checking, analyzing, authorizing, reconciling, supervising, reviewing, segregating, and following-up. Control activities are not limited to traditional accounting processes. For example, a hospital will provide secure storage for dangerous drugs, and a chemical company will balance bulk liquid chemicals to records periodically as part of its routine inventory control system.

99 Control activities also include those activities designed to ensure the completeness, accuracy and availability of information. There are some specific control activities for the information-systems environment such as logical and physical access restrictions, back-up and recovery, job scheduling and completion checks, system edits and software selection and testing.

Documentation

100 Control activities and related policies and procedures (the steps required to perform an activity) may be communicated informally or documented formally in manuals. In some cases, they may not require documentation because they are well understood, or relatively simple, or involve very few people.

101 In other cases, the cost of formal documentation is worth the benefits, which include consistency across units, locations and functions within the organization. Another benefit of documentation is that it provides the basis for continuity despite personnel changes. The legal and regulatory environment in which the organization operates, as well as customer requirements, may also influence the extent to which control activities and procedures are formally documented.

MONITORING AND LEARNING

Monitoring and Learning groups criteria that provide a sense of the organization's evolution. They address:

- monitoring internal and external environments
- monitoring performance
- challenging assumptions
- reassessing information needs and information systems
- follow-up procedures
- assessing the effectiveness of control

D1 External and internal environments should be monitored to obtain information that may signal a need to re-evaluate the organization's objectives or control.

102 Changes in external conditions (such as changes in competitive conditions, regulations, social trends and technology) can have a significant effect on an organization's ability to meet its objectives. Such changes can alter what shareholders, customers and other stakeholders expect from the organization, and the risks and opportunities it faces.

103 Monitoring the external environment can provide valuable information on the state of the internal environment. For example, soliciting comments from customers is a way of monitoring the effectiveness of policies directed at customer satisfaction. Contact with customers or suppliers may identify breaches of a code of conduct, deficiencies, or areas that are particularly effective.

104 To a large extent, management can initiate or control changes to the internal environment. Nevertheless, it can change unexpectedly. For example, employee attitudes may change in unexpected ways in response to management initiatives or external circumstances. Monitoring may involve the use of confidential surveys, workshops, or less formal means.

105 Changes to any aspect of an organization will have consequences for control. For example, a reorganization may affect morale, application of policy or the performance of control activities. During and after such changes, specific monitoring may be advisable to determine whether control should be strengthened.

106 Continuously monitoring the external and internal environments enables the organization to diagnose changes early and respond to them promptly. Unexpected change poses a more significant risk than change that has been anticipated, because the organization may not be prepared to respond to threats and opportunities.

107 Information gained through monitoring environments may signal a need to re-evaluate the organization's objectives or other aspects of the organization. Objectives may need to be adjusted to respond to changed opportunities. Such adjustments may require a change to other aspects of the organization, including its control elements. Information gained through monitoring environments may also signal a need to alter the organization even if current objectives are not adjusted.

D2 Performance should be monitored against the targets and indicators identified in the organization's objectives and plans.

108 Monitoring operating performance offers an opportunity to learn from experience. If progress toward objectives is faster or slower than planned, underlying factors may indicate a need to revise objectives or to otherwise redirect or refocus the organization. For example, poor performance may reflect technological or financial disadvantages, and may require changes to objectives or plans relating to technology, markets or production plans.

109 To monitor operating performance, people need to have timely, reliable information on operating results. Operating performance is usually monitored by the unit responsible for results and by those to whom the unit is accountable.

110 The targets and indicators used in monitoring usually change as the related objectives change. Other alterations may be required when the targets or indicators change. For example, data sources may be different or new, or different reports and analysis may be required.

111 The performance of control activities also requires monitoring. Such monitoring may detect and allow for correction of design and performance problems. Such problems might occur if the activities have become obsolete or lost effectiveness, or if alternative control activities have become more cost effective. Training or performance issues may also be identified.

112 The formality of the monitoring process will vary by size and type of organization. In large organizations it may include detailed reporting and analysis. Smaller organizations may have a less elaborate process since senior management is likely to be more involved in the performance being monitored.

D3 The assumptions behind an organization's objectives should be periodically challenged.

113 An organization's objectives, and the control elements that support their reliable achievement, rest on fundamental assumptions about how its world works. For example, strategic objectives may rest on assumptions about market demand, competitive conditions and the speed of technological developments.

114 Assumptions about "how the system works" are often widely held in an organization, yet people may be unaware of them. Such unconscious assumptions can inhibit the ability to adapt to change because they lead people to screen out information that does not fit their preconceptions. Open dialogue is necessary to identify assumptions.

115 If an organization's assumptions are invalid, control may be ineffective. For example, organizational values may rest on assumptions about people that no longer hold true because of changes in the work force. The selection of performance indicators to be monitored may rest on assumptions about demand that are no longer valid because substitute products or new technology have changed the market. Periodically challenging the organization's assumptions is key to the effectiveness of control.

D4 Information needs and related information systems should be reassessed as objectives change or as reporting deficiencies are identified.

116 As an integral part of control, monitoring is ultimately directed at the organization's objectives. When objectives change, information needs may also change. Those who need the information and those responsible for gathering it need to communicate with each other to ensure needs are understood and met in a timely and efficient manner. Since organizations operate in changing environments with changing objectives, information systems usually require change over time as well.

117 Deficiencies in reporting may be identified from users' comments or from specific control activities. Failure to receive expected information may lead to a review of information-gathering and reporting processes in the area. The correction of deficiencies may require changes in the information being gathered, the way it is gathered, the content of reports or the related information systems.

D5 Follow-up procedures should be established and performed to ensure appropriate change or action occurs.

118 An organization needs to change if control is to remain effective. The consideration of the information produced by monitoring all aspects of performance should lead people to learn what improvements are required. The changes may be to objectives or plans, in order to take advantage of an opportunity or to react to a threat; to control activities, in order to respond to a change in circumstances, such as a new process or technology; or to information systems, in order to respond to changing objectives or new information needs. This constant change enables the organization to modify its outputs and thereby survive and prosper in a constantly changing environment.

119 For change to be effective, information such as the results of control assessments must be communicated to those who can authorize change. If this authority is centralized, communication with the individuals responsible for performing and assessing the activities that are to be changed is important to gain their acceptance and to ensure that gaps or constraints are not overlooked.

120 Wherever key changes or actions are to be implemented, follow-up should confirm that they are carried out. Where change is particularly rapid or short-lived, regular monitoring processes may need to be supplemented by special arrangements.

121 Follow-up occurs at various levels throughout the organization. The board of directors (or its equivalent), would expect to be told whether action or change initiated or supported by them has actually occurred. Other individuals and groups within the organization would similarly require information about the implementation of actions or changes they have initiated.

D6 Management should periodically assess the effectiveness of control in its organization and communicate the results to those to whom it is accountable.

122 A periodic review of the effectiveness of control in the organization takes a broader and more integrated approach than the assessment of control within a unit of the organization. The effectiveness of control in an organization is different from the sum of the effectiveness of control within each unit because the organization includes the dynamic interaction of its various elements. The frequency and depth of the review will vary depending on the nature and significance of the objective and the related risks.

123 The scope of an assessment of control can be tailored to meet particular needs. For example it may address all of the corporate objectives approved by the board of directors, or only certain ones specified by the board.

124 The assessment of control in an organization can be conducted in a number of ways: informally, for example through direct contact; in a more formal and organized fashion, for example by using control experts such as auditors trained in observation and interview techniques; or by self-assessment, whereby groups assess the effectiveness of control in their own operations. Exhibit C sets out examples of questions that could be used in such an assessment.

125 Regardless of how the assessment is conducted, its results should be reported to complete the accountability loop to those responsible for the organization as a whole. For example, within a corporation this is the board of directors, or its equivalent. Such reporting may be combined with periodic reporting of the discharge of operating responsibility.

Exhibit C
SAMPLE ASSESSMENT QUESTIONS

To assess the effectiveness of control, an organization may find it helpful to express the criteria as questions tailored to its circumstances. The following is a simple example of questions a group might use to conduct a self-assessment. They have been tailored by drawing on some of the explanatory material in this guidance. In each case, the answer to the question would be followed up by "How do we know" to trigger identification and discussion of the control processes.

Purpose

- Do we clearly understand the mission and vision of the organization?
- Do we understand our objectives, as a group, and how they fit with other objectives in the organization?
- Does the information available to us enable us to identify risk and assess risk?
- Do we understand the risk we need to control and the degree of residual risk acceptable to those to whom we are accountable for control?
- Do we understand the policies that affect our actions?
- Are our plans responsive and adequate to achieve control?
- Do we have manageable performance targets?

Commitment

- Are our principles of integrity and ethical values shared and practised?
- Are people rewarded fairly according to the organization's objectives and values?
- Do we clearly understand what we are accountable for, and do we have a clear definition of our authority and responsibilities?
- Are critical decisions made by people with the necessary expertise, knowledge and authority?
- Are levels of trust sufficient to support the open flow of information and effective performance?

Capability

- Do we have the right people, skills, tools and resources?
- Is there prompt communication of mistakes, bad news and other information to people who need to know, without fear of reprisal?
- Is there adequate information to allow us to perform our tasks?
- Are our actions coordinated with the rest of the organization?
- Do we have the procedures and the processes to help ensure achievement of our objectives?

Monitoring and Learning

- Do we review the internal and external environment to see whether changes are required to objectives or control?
- Do we monitor performance against relevant targets and indicators?
- Do we challenge the assumptions behind our objectives?
- Do we receive and provide information that is necessary and relevant to decision-making?
- Are our information systems up to date?
- Do we learn from the results of monitoring and make continuous improvements to control?
- Do we periodically assess the effectiveness of control?

Appendix 1

COMPARISON TO COSO

The "Internal Control – Integrated Framework" document produced by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) is becoming an accepted reference on control in the United States. The guidance in this document builds on the concepts in the COSO document. While there are large areas of overlap and consistency between the two documents, they differ in some respects.

The principal differences between the two documents are set out below. The practical effect of these differences in a particular situation would depend on how either one was interpreted and applied. However, it is the belief of the Criteria of Control Board (CoCo) that organizations that follow this guidance will have thereby considered the components of the COSO framework.

Definition and scope

COSO defines internal control as "a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations.
- Reliability of financial reporting.
- Compliance with applicable laws and regulations."

CoCo defines control as "those elements of an organization (including its resources, systems, processes, culture, structure and tasks) that, taken together, support people in the achievement of the organization's objectives." It defines three categories of objectives:

- Effectiveness and efficiency of operations.
- Reliability of internal and external reporting.
- Compliance with applicable laws and regulations and internal policies.

Consistent with its definition, CoCo includes within the scope of control some particular aspects of management that COSO excludes: objective setting, strategic planning and risk management, and corrective actions. CoCo excludes from the scope of control only decision-making. (References: COSO Framework page 17, CoCo paragraphs 8–9).

Underlying concepts

CoCo is explicit about some concepts that are not explicitly addressed in COSO. These are:

(a) Control includes the identification and mitigation of the risk of failure to maintain the organization's capacity to identify and exploit opportunities. (Paragraph 7)

(b) Control includes the identification and mitigation of the risk of failure to maintain the organization's resilience – its capacity to respond and adapt to unexpected risks and opportunities, and to make decisions on the basis of telltale indications in the absence of definitive information. (Paragraph 7)

(c) CoCo includes two criteria not explicitly addressed in COSO. They relate to mutual trust between people (B4) and the periodic challenge of assumptions (D3). In addition, the concept of monitoring in this CoCo guidance includes monitoring of the operating performance of the organization. COSO's discussion of monitoring could be interpreted to be focused on monitoring of specific control activities.

The judgment of effectiveness

COSO addresses this as follows: "Internal control can be judged effective in each of the three categories, respectively, if the board of directors and management have reasonable assurance that:

- They understand the extent to which the entity's operations objectives are being achieved.
- Published financial statements are being prepared reliably.
- Applicable laws and regulations are being complied with.

Determining whether a particular internal control system is effective is a subjective judgment resulting from an assessment of whether the five components (control environment, risk assessment, control activities, information and communication, and monitoring) are present and functioning effectively. Their effective functioning provides the reasonable assurance regarding the achievement of one or more of the stated categories of objectives. Thus, these components are also criteria for effective internal control." (COSO Framework page 16)

CoCo differs in three important respects:

(a) The judgment of effectiveness is made in relation to a specific objective (such as customer service levels), not a category of objectives (such as effectiveness and efficiency of operations).

(b) CoCo asks that an assessment of the effectiveness of control be made against twenty specific criteria. COSO asks that the assessment be made for each of five components, and provides illustrative "issues to consider" for each component. All of COSO's "issues to consider" are addressed directly or indirectly within the CoCo document, except perhaps the following:

- Receptivity of management to employee suggestions of ways to enhance productivity, quality or other similar improvements.
- Extent to which personnel, in carrying out their regular activities, obtain evidence as to whether the system of internal control continues to function.
- Extent to which outside parties have been made aware of the entity's ethical standards.
- Extent to which training seminars, planning sessions and other meetings provide feedback to management on whether controls operate effectively.
- Appropriateness of the level of documentation (of an evaluation).

(c) CoCo includes the following definition of effective control: Control is what makes an organization reliable in achieving its objectives. Control is effective to the extent that it provides reasonable assurance that the organization will achieve its objectives. Or, stated another way, control is effective to the extent that the remaining risks of the organization failing to meet its objectives are deemed acceptable. (Glossary)

* * * * * * * * * * *

CoCo's criteria can be regrouped into different structures. The following table shows how they can be regrouped into the five-component structure of COSO.

CoCo criteria of control regrouped into COSO components

Control Environment

B1 Shared ethical values, including integrity, should be established, communicated and practised throughout the organization.

B2 Human resource policies and practices should be consistent with an organization's ethical values and with the achievement of its objectives.

B3 Authority, responsibility and accountability should be clearly defined and consistent with an organization's objectives so that decisions and actions are taken by the appropriate people.

B4 An atmosphere of mutual trust should be fostered to support the flow of information between people and their effective performance toward achieving the organization's objectives.

C1 People should have the necessary knowledge, skills and tools to support the achievement of the organization's objectives.

Risk Assessment

A1 Objectives should be established and communicated.

A2 The significant internal and external risks faced by an organization in the achievement of its objectives should be identified and assessed.

A5 Objectives and related plans should include measurable performance targets and indicators.

D1 External and internal environments should be monitored to obtain information that may signal a need to re-evaluate the organization's objectives or control.

Control Activities

A3 Policies designed to support the achievement of an organization's objectives and the management of its risks should be established, communicated and practised so that people understand what is expected of them and the scope of their freedom to act.

C4 The decisions and actions of different parts of the organization should be coordinated.

C5 Control activities should be designed as an integral part of the organization, taking into consideration its objectives, the risks to their achievement, and the inter-relatedness of control elements.

Information and Communication

C2 Communication processes should support the organization's values and the achievement of its objectives.

C3 Sufficient and relevant information should be identified and communicated in a timely manner to enable people to perform their assigned responsibilities.

A4 Plans to guide efforts in achieving the organization's objectives should be established and communicated.

D4 Information needs and related information systems should be reassessed as objectives change or as reporting deficiencies are identified.

Monitoring

D2 Performance should be monitored against the targets and indicators identified in the organization's objectives and plans.

D3 The assumptions behind an organization's objectives should be periodically challenged.

D5 Follow-up procedures should be established and performed to ensure appropriate change or action occurs.

D6 Management should periodically assess the effectiveness of control in its organization and communicate the results to those to whom it is accountable.

Appendix 2

COMPARISON OF A TOTAL QUALITY MANAGEMENT APPROACH TO THIS CONTROL FRAMEWORK

An organization may have adopted a management approach which has its own routines and vocabulary. Applying a control framework does not mean that these must be thrown out wholesale. Instead, the current management approach can be compared to the control framework and modified as necessary to improve control.

This appendix shows a comparison between the control framework in this guidance and the Baldrige Award Criteria.[5] The comparison shows where the two sets of criteria particularly overlap.

The comparison also shows that some of the control criteria are not addressed in the Baldrige quality criteria. Identification of overlaps and gaps at this level permits an organization to consider in detail the extent to which its management approach may need to be revised to address both sets of criteria.

Omitted from the comparison are the Baldrige criteria that call for data on results.

[5] American Society for Quality Control, Milwaukee, 1994.

Baldrige Award Criteria	A1	A2	A3	A4	A5	B1	B2	B3	B4	C1	C2	C3	C4	C5	D1	D2	D3	D4	D5	D6
Leadership																				
Senior Executive Leadership						✓					✓									
Management for Quality	✓							✓												
Public Responsibility and Corporate Citizenship			✓			✓					✓				✓					
Information and Analysis																				
Scope and Management of Quality and Performance Data and Information												✓		✓				✓		
Competitive Comparisons and Benchmarking					✓										✓					
Analysis and Uses of Company-Level Data												✓						✓		
Strategic Quality Planning																				
Strategic Quality and Company Performance Planning Process				✓																
Quality and Performance Plans				✓																
Human Resource Development and Management																				
Human Resource Planning and Management				✓							✓									
Employee Involvement								✓												
Employee Education and Training											✓									
Employee Performance and Recognition							✓													
Employee Well-Being and Satisfaction										✓										
Management of Process Quality																				
Design and Intoduction of Quality Products and Services	✓													✓						
Process Management: Product and Service Production and Delivery Processes														✓						
Process Management: Business and Support Service Processes														✓						
Supplier Quality	✓										✓			✓						
Quality Assessment																				✓
Customer Focus and Satisfaction																				
Customer Expectations: Current and Future															✓					
Customer Relationship Management					✓															
Commitment to Customers	✓										✓			✓						
Customer Satisfaction Determination															✓					
Not addressed in Baldrige Criteria		✗							✗				✗			✗	✗		✗	

This book is printed on recycled paper and both the text and cover contain
a minimum of 50% recycled fibre, including 10% post-consumer fibre.
Environmentally friendly canola or soya-based inks have been used.