

Evaluating Internal Control Systems

A Comprehensive Assessment Model (CAM)
for Enterprise Risk Management

Carolyn Dittmeier, CIA, CRMA

Paolo Casati, CIA, CRMA



Copyright © 2014 by The Institute of Internal Auditors Research Foundation (IIARF). All rights reserved.

Published by The Institute of Internal Auditors Research Foundation, 247 Maitland Avenue, Altamonte Springs, Florida 32701-4201

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form by any means—electronic, mechanical, photocopying, recording, or otherwise—without prior written permission of the publisher. Requests to the publisher for permission should be sent electronically to: bookstore@theiia.org with the subject line “reprint permission request.”

The IIARF also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books. For more information about IIARF products, visit our website at www.theiia.org/bookstore.

Limit of Liability: The IIARF publishes this document for informational and educational purposes and is not a substitute for legal or accounting advice. The IIARF does not provide such advice and makes no warranty as to any legal or accounting results through its publication of this document. When legal or accounting issues arise, professional assistance should be sought and retained.

The Institute of Internal Auditors’ (IIA’s) International Professional Practices Framework (IPPF) comprises the full range of existing and developing practice guidance for the profession. The IPPF provides guidance to internal auditors globally and paves the way to world-class internal auditing.

The IIA and The IIARF work in partnership with researchers from around the globe who conduct valuable studies on critical issues affecting today’s business world. Much of the content presented in their final reports is a result of IIARF-funded research and prepared as a service to The IIARF and the internal audit profession. Expressed opinions, interpretations, or points of view represent a consensus of the researchers and do not necessarily reflect or represent the official position or policies of The IIA or The IIARF.

ISBN-13: 978-0-89413-879-9

20 19 18 17 16 15 14 1 2 3 4 5 6 7 8 9



CONTENTS



Introduction	6
Fundamentals of Risk Management and Internal Control	10
A Single Defined Framework	10
Strong Communication of Business and Governance Objectives	11
Evaluating Risks: A Comprehensive, Cross-Functional Approach	13
The Comprehensive Assessment Model	14
Scope and Benefits	14
Risk-Based Approach	15
Risk Mitigation/Control Objectives	15
Attributes and Characteristics of Internal Controls	18
Complementarity with the COSO Models	19
Assessing Risk-Based Internal Controls	19
Overview of the Assessment Criteria	20
Criteria to Assess the Design of Internal Controls	21
Performance or Effective Functioning of the Internal Control System	38
Evaluation of the Cost-Benefit Factor of Controls	44
Control Assessment Methodology	46
Objective Assessment through Quantitative vs. Qualitative Approach	47
Assessment Methodology for Each Internal Control	47
Evaluation of the Internal Control System of an Overall Business Process	50
Expressing an Opinion on the Internal Control System of a Full Process	52
Business Case	53
Enterprise-Level Assessment	58
Notes	60
The IIA Research Foundation Sponsor Recognition	61
The IIA Research Foundation Board of Trustees	63
The IIA Research Foundation Committee of Research and Education Advisors	64



LIST OF EXHIBITS



Exhibit 1.1:	Business and Governance Objectives Tailored to Process Objectives .	12
Exhibit 1.2:	Exemplary Risk Model	13
Exhibit 1.3:	Internal Risk Categories	14
Exhibit 2.1:	Risk Mitigation and Control Objectives	16
Exhibit 2.2:	Risk Weight	17
Exhibit 2.3:	Control Process	18
Exhibit 3.1:	Comprehensive Assessment Model (CAM)	21
Exhibit 3.2:	Assessment of Internal Control	23
Exhibit 3.3:	Internal Control Case Study.	24
Exhibit 3.4:	Level of Discretion	25
Exhibit 3.5:	Discretion Example	25
Exhibit 3.6:	Segregation	26
Exhibit 3.7:	Level of Segregation	27
Exhibit 3.8:	Segregation Example.	28
Exhibit 3.9:	Level of Independence	29
Exhibit 3.10:	Independence Example	29
Exhibit 3.11:	Integrative Control Factors	30
Exhibit 3.12:	Integrative Control Example	31
Exhibit 3.13:	Level of Automation.	32
Exhibit 3.14:	Automation Example	32
Exhibit 3.15:	Level of Adaptability	33
Exhibit 3.16:	Adaptability Example.	34
Exhibit 3.17:	Level of Traceability	35
Exhibit 3.18:	Traceability Example	35
Exhibit 3.19:	Control Performance	36
Exhibit 3.20:	Level of Timeliness	37
Exhibit 3.21:	Timeliness Example.	37
Exhibit 3.22:	Level of Coverage	38
Exhibit 3.23:	Level of Availability	39
Exhibit 3.24:	Assessing Criteria	41



Exhibit 3.25:	Level of Compliance	42
Exhibit 3.26:	Measuring Residual Risk	43
Exhibit 3.27:	Cost-Benefit Factor	46
Exhibit 4.1:	Control Strength	47
Exhibit 4.2:	Assessment of Control	49
Exhibit 4.3:	Control Objectives	51
Exhibit 4.4:	Overall Process	52
Exhibit 4.5:	Overall Process Assessment	53
Exhibit 5.1:	Standard Production Time	54
Exhibit 5.2:	Control Production Time	55
Exhibit 5.3:	Internal Control Production Standards	56
Exhibit 5.4:	Internal Control Annual Review	57
Exhibit 5.5:	Inadequate Control	58
Exhibit 6.1:	Assessment Process	59

INTRODUCTION

The Comprehensive Assessment Model (CAM) is an innovative methodology that provides for *integrated assurance*. This assurance is based on the evaluation of control and risk management processes, considering all pertinent business and governance objectives, through a unified and unique assessment approach.

The CAM approach is both objective and structured, providing the internal audit profession with the particular advantage of promoting full integration of entity objectives. Once fully implemented, CAM will allow for entity-level opinions useful for audit committee assurance as well as for corporate governance reporting required under international stock exchange regulation and recommendations.¹

Today's audit committee wrestles with the need to ensure complete and efficient oversight over internal governance. Oversight is frequently fragmented between compliance, reporting, and operational objectives. For this reason, internal audit planning is often divided into several types of auditing (management, fraud, IT, operational, financial). Thus, assurance over the enterprise risk model framework is also fragmented.

By its nature and mission, internal audit is intended to provide assurance for the overall adequacy of the internal governance system and may be the primary user of CAM. Presenting the criteria of this model to the audit committee or board propels the profession forward by providing a solid, reliable foundation for ensuring effective oversight.

In the authors' opinion, CAM is fully aligned with the Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) enterprise risk management (ERM) and internal control models. It is also intended to be one of the primary measures supporting the three lines of defense model.²

CAM offers innovative ideas for the internal audit profession in truly applying The Institute of Internal Auditors' (IIA's) definition of internal auditing as an "independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to *evaluate and improve the effectiveness of risk management, control, and governance processes.*" In support of this, the key attribute of CAM is its objective, systematic approach. Parameters may be flexible while maintaining structure and consistency in application. For this reason, this methodology guarantees true *objectivity* in the assurance activity.

The methodology provides a way to measure internal controls. It does so in a way that is strictly in correlation to the risk mitigation/control objectives that support the relevant business and governance goals of the process.

Eleven business and governance objectives encompass all ERM goals:

1. Market share or growth
2. Client satisfaction
3. Volume
4. Cost containment
5. Quality

6. Innovation and technology
7. Profitability
8. Information reliability (i.e., accounting or management)
9. Legal
10. Security
11. Social responsibility

These objectives can be drilled down to process level, and the risk mitigation objectives can be categorized so that all risks can be completely identified. The objectives may be weighted accordingly, based on risk-assessment techniques.

While the objectives are established in a top-down approach, the subsequent assessment of the internal controls calls for a bottom-up approach. The methodology is also aligned to the valuable internal audit approach of evaluating risk management and internal control systems on a process basis. It thereby cuts across the various business units, following the various sub-phases necessary to achieve the process deliverables.

CAM makes a firm distinction between assessing the system's architecture or *design* and its effective *performance* or functioning. The overall assessment is a combination of both; however, the evaluation of an internal control system's effective performance must be based on its design assessment. If the design is inadequate, it may not even be appropriate to proceed with the performance assessment because of cost-benefit factors. Alternatively, performing compliance audits based on formal procedures without a structural design analysis allows for a clear risk of error and *audit risk*, which is unacceptable for overall assurance goals.

In addition, CAM provides clarity on the important and essential components of an *internal control*. A control must have:

- Some sort of expected result, whether a formalized standard or a managerial expectation
- A way to gather information about the actual situation
- A way to compare the actual with expectations
- A way to react to deviations

This simple definition is fundamental in considering whether controls are effective. It is demonstrated further in the model's assessment criteria.

The following criteria are measured to assess the internal control system's *design*. First, it measures the degree to which the assigned controls are:

- Relevant or capable of responding to specific business and governance objectives
- Capable of mitigating the intended risks
- Reflective of control process completeness, as previously defined

Next, it considers:

- Degree or extent of set expectations
- Process/existence of situational data collection
- Review, comparison, and correction process

Criteria that indicate a fault in the internal control system's design include, but are not limited to:

- Information without indication of a true correction process
- Control based on poor/no standards
- Control that captures just partial information about a defective process

Additional evaluation criteria include:

- *Level of coverage* of all risks associated with the identified business and governance objectives

Note: This criteria brings out the value of an integrated assessment model.

- *Strength* of the selected controls based on several factors, including:
 - Independence of those accountable for the control activity
 - Independence of information sources used for control
 - Segregation of roles
 - Extent of IT automation
 - Traceability
 - Ability to guarantee the control, even in fluctuating volumes of activity

Note: These are illustrated in detail in this report.

- *Timeliness* of the controls in responding to negative events, which further assesses the ability of the control to correct a problem prior to worst-case scenario (e.g., promptly address quality control after customer complaint, preventing customer loss; IT control address security attack in real time rather than after loss/infection)

The following elements should be assessed to evaluate the effective performance of internal controls:

- Availability of resources needed to perform the controls (for example, financial [available budget], technical [available/maintained tools], and human resources (HR) [allocated employees])

- Compliance with the established control design

Note: While this concept is well understood in traditional auditing, it represents a fraction of the significant control criteria presented in this report.

- Activities to monitor residual risks

Controls are not intended to eliminate risks, but rather mitigate them. As such, residual risk levels must be monitored to ensure that they are consistent with acceptability and tolerance levels identified in the original control design. When risk levels are disproportionate, the design elements themselves must be revisited.

Finally, the balance of cost and benefit is considered when evaluating the *economic/efficiency* factors of internal controls. An internal control system that effectively and efficiently presides over the mitigation of risk depends on the ability to select optimal control solutions among multiple alternatives. However, *optimization* can only be evaluated if the cost of control is properly measured. It must be based on direct and indirect cost factors. It should also consider whether the organization has an adequate risk measurement process in place to analyze benefit, opportunity, and risk.

CAM is flexible, as it facilitates the development of personalized guidelines for implementing the above criteria. This may evolve over time, even with the maturity scale of the model's implementation. The model incorporates *risk weightings* to account for the relative significance of the underlying business and governance objectives, as well as the related potential risks that may impact the process.

In summary, the CAM provided in this report encompasses the concept of combined assurance by truly taking into account all ERM objectives in an integrated manner. It uses an all-inclusive, comprehensive set of criteria and assessment methodology from process level to entity level.

One of the businesses that successfully tested the implementation of CAM is Poste-Italiane, a large, diversified enterprise operating in financial services, logistics, communication, and IT services. Its diversification strategy led to nomination as a *Fortune* Most Admired Company in 2013. However, it is a challenge for any internal audit department to provide global assurance with limited resources. The audit universe consisted of multiple selling channels and multiple products that converged into a business process model of approximately 300 major processes. The processes were identified at group level and then classified under business, governance, support, and resource management categories.

In this business case, 26 risk mitigation objectives were identified against the 11 previously mentioned business and governance goals. Internal audit was trained in the methodology. Additionally, a support system was implemented for mapping processes containing risk mitigation objectives and the model's control assessment criteria. Assessment guidelines were formed and implemented for all audits following the model's pilot stage.

In the initial phase of each audit, management collaborated to determine the process subject's pertinent business and governance objectives. This clearly established relevant risk mitigation/control objectives for the assessment that follows.

- Audit reports produced an overall assessment of the process internal control system on a scale of 1 to 5. The system's strengths and weaknesses were readily understandable and analyzed through the model's inherent structure.
- Process consolidation and full implementation took place over two years. The evaluation of the internal control design allowed for the creation of efficient and effective audit programs to be implemented on a standardized basis (through the wide retail network) to test its effective functioning of controls as well as *residual risks* identified.

The progressive coverage allowed for overall assessments of broad processes and led to the entity-level assessment process, which was successfully presented to the audit committee. From this and other business cases shared with chief audit executives (CAEs), we believe that CAM's potential contribution to the internal audit profession, as well as to board governance, is enormous.

FUNDAMENTALS OF RISK MANAGEMENT AND INTERNAL CONTROL

Before entering into the specific methodology of the CAM, it is important to highlight what are considered to be the essential macro-organizational elements behind sound internal governance. Consideration of these elements helps the board, audit committee, and management understand:

- The positioning of the organization within the maturity scale of governance
- The overall internal environment, as contemplated by ERM
- Attributes of the organization, which will be useful for the specific analyses within CAM

The following three elements are intended to ensure an integrated, effective, efficient, and cost-effective internal governance:


1. A single, defined framework for the risk management and internal control system of the enterprise
2. Strong communication of business and governance objectives, which allow for the definition of appropriate and balanced risk mitigation or control objectives for each process
3. A comprehensive cross-functional approach to evaluating risks and controls

In addition, the evaluation of the risk management and internal control systems on an integrated, objective basis is essential. This includes considering all business and governance objectives at both the process and entity levels.

The methodology presented in this report allows the audit committee and internal audit to provide global assurance of the overall risk management and internal control system—in an objective manner—which is strongly aligned with the objectives set by the organization.

A SINGLE DEFINED FRAMEWORK

While risk management and internal control frameworks have been developed successfully³ on a conceptual basis, they have only been partially implemented. Such frameworks are useful for providing a conceptual structuring of the internal control system components. It is essential that the board and the organization adopt an overall framework. It should be the premise for the specifications



of formal procedures, frequently cited as requirements within legislation and regulations. A framework allows for uniformity of governance terminology, as well as a top-down approach to risk management; it officially breaks down the paradigm of “control through procedures.”

The ERM⁴ framework is intended to guarantee a structured approach for identifying and measuring effective risk levels in all areas of an organization (e.g., from strategic to operational, from compliance to business, etc.). However, based on the corporate governance reports of listed companies, the ERM framework has not been widely adopted globally.

To be successful, the framework must be implemented to the point that risk management policies and control objectives are progressively embedded in the control activities at all levels. Those objectives must be defined strategically and drilled down to process level. This should include the organization’s incentive/disincentive management system.

The subsequent sections of this report provide a way to measure the controls in correlation to the risk mitigation and control objectives⁵ that drive the specific business and governance goals of the process. While the objectives are established from a top-down approach, the subsequent assessment of internal control is generally performed bottom-up.

The foundations of the risk management and control environment, as well as general governance mechanisms (referred to as the *internal environment* in the ERM framework), are also represented by processes (e.g., HR, organization, strategic planning), which should be subjected to the same evaluation methodology. This helps capture all critical elements (e.g., strength, timeliness, coverage, etc.).

STRONG COMMUNICATION OF BUSINESS AND GOVERNANCE OBJECTIVES

As expressed in the ERM framework, the communication of objectives is essential to an appropriately functioning internal control system. At top level, this includes developing an explicitly objective strategic plan with an integrated, top-level risk management process.

Without adequate communication of objectives, the priorities of the individual departments or functions that contribute to the process may differ or conflict. For example, the accounting function’s objective of accuracy may conflict with the necessary availability of information for customer relations management. Likewise, the priority of cost containment within the purchasing department may hamper or preclude the equally important objective of timeliness with regard to the organization’s purchasing and investment needs.

Exhibit 1.1 shows an example of how business and governance objectives at the enterprise level are tailored to the process objectives. From there, risk assessment, mitigation, and control objectives can be defined appropriately.

Exhibit 1.1: Business and Governance Objectives Tailored to Process Objectives

Enterprise Level	Process-Level Manufacturing	Process-Level Financial Services
Business Objectives:		
1. Volume	1. Capacity planning	1. Increase transaction volume
2. Cost Containment	2. Cost containment	2. Minimize overhead
3. Process Effectiveness	3. Production quality	3. Servicing capability
4. Customer Satisfaction	4. Time to market	4. Minimize customer claims
5. Profitability	5. -	5. Profitability of financial service product
6. Innovation/Technology	6. Plant technology	6. Information systems
7. Market Share	7. -	7. Increase customer base
Governance Objectives:		
8. Information Reliability	8. Reliable control reports	8. Reliable accounting and management reporting
9. Legal Compliance	9. Compliance to bid regulation	9. Compliance to financial sector regulations
10. Security	10. Worker's safety	10. Information security
11. Social Responsibility	11. Pollution containment	11. -

Thus, the organization promotes clarity in objectives by referencing a defined goal model. It sets the stage for appropriate risk assessment in strict correlation to the objectives and ensures full consideration of:

- The business objectives in terms of maximizing revenues, cost containment, product or service quality, retention or increase of market share, customer satisfaction, etc.
- The governance objectives such as legal compliance, reliability of information, employee welfare, environmental safety, and other social values

In turn, without an explicit understanding of these objectives, risk management is hampered.

As mentioned, risk management and control objectives for a given process can sometimes conflict. Therefore, a balanced approach toward diversified objectives must be found through risk assessment, weighting control objectives accordingly.

EVALUATING RISKS: A COMPREHENSIVE, CROSS-FUNCTIONAL APPROACH

As a key element of the governance processes, risk assessment must:

- Guarantee full coverage of the organization’s significant risks
- Adopt approaches to identifying risks, which ensure a clear correlation to the organization’s objectives, both business and governance
- Promote an appropriate and proportionate allocation of resources to control activities and the control functions dedicated to monitoring risks based on importance

Thus, the models applied in identifying risks must be exhaustive. They must not be conditioned by excessive focus related to regulatory or other specialized issues. Regulations have sometimes focused attention on single-risk areas (e.g., business sector, legal, etc.), responding to regulatory pressures and negative business events. This focus, however, can result in disproportionate attention and allocation of resources to such risks with respect to other nonregulated risk areas.

Of course, risk assessment differs from one organization to the next. Furthermore, prioritizing the allocation of resources to control those risks is subject to legal regulation. If that regulation is not considered in a comprehensive framework, it can impede the overall risk management of the organization and cause inefficiencies in resource management. The end result is an imbalanced risk management process.

As a simple reminder of the *broadness* of risk categories, an exemplary model is illustrated in exhibits 1.2 and 1.3. However, any model can be associated with the strategic, compliance, operational, and financial objectives called for under the enterprise risk framework.

Exhibit 1.2: Exemplary Risk Model (strategic, compliance, operational, and financial)
External Risk Categories
Negative financial and macroeconomic conditions
Negative market trends
Negative customer trends
Competing emerging technologies
Legal or regulatory changes
Natural events
External attacks

Exhibit 1.3: Internal Risk Categories

Internal Risk Categories
Conflicting or defective strategic or operational objectives
Poor quality of human resources (lack of commitment, fraud, etc.)
Lack of resources (financial, human, technological)
Errors

Thus, the process for assessing the risks must take place at entity level. Single organizational functions dedicated to the assessment of specialized risks must be placed within a single enterprise risk process. This process must also prioritize risks based on their correlation to the entities' objectives, considering:

- The extent to which the combination of risks potentially impacts each objective
- Or, alternatively, the impact of certain risks on multiple entity objectives

The need for a cross-functional approach to evaluating risks generally calls for a delineation of the organization by end-to-end processes based on the organization. Business process models create the basis for cross-functional risk management and offer the appropriate basis for audit universe and strategic audit planning.

The organization should evaluate the risk management and internal control systems process by process across the various business units and through process phases/activities. The primary basis for evaluating the internal control and risk management systems should not be the evaluation of the appropriate function of single units and control responsibilities.

THE COMPREHENSIVE ASSESSMENT MODEL

SCOPE AND BENEFITS

An efficient and effective internal control system, which presides over the mitigation of risk, depends upon the ability to analyze numerous options and ultimately select the control solutions that optimize cost and benefit.

The cost of internal control systems is an increasingly vital issue. Therefore, a single, consistent, and comprehensive way to evaluate internal controls must be found. The approach presented here for evaluating internal control systems, including the risk management processes, is innovative. It has been successfully tested within complex business environments⁶ and is based on the following foundations:

- a. The evaluation of internal control must make a firm distinction between assessing the architecture/design of the system and measuring the effective performance/functioning of the system. The overall assessment of the internal control system will be a combination of the conclusions in both areas.

- b. A system that is poorly designed leaves more room for undesirable residual risks than a well-designed internal control system, after taking into account the risk appetite and risk management strategies. For this reason, if a system's design is inadequate, it may not be cost-beneficial to proceed assessing its performance until it is revised and strengthened.
- c. The evaluation of the architecture or design of the internal control system should consider all pertinent risk mitigation/control objectives. It should evaluate the controls designed to achieve the objectives, process by process, including:
 - The relevance of existing controls, their capability to preside over the specific business and governance objectives, and the means to identify deviations from expected results and correct the process
 - The completeness of coverage—by the controls—of identified risks in relation to the specific business and governance objectives
 - The timeliness of the controls in responding to negative events
 - The strength of the selected controls, based on several factors
- d. The evaluation of the effective performance of the system will depend upon:
 - The availability of resources needed to perform the controls
 - Compliance with the established control design
 - Activities to monitor residual risks
- e. The evaluation of the economic and efficiency factors of the controls

RISK-BASED APPROACH

As mentioned, the methodology of evaluating an internal control system is founded on risk-based concepts. It calls for the identification and preliminary assessment of external and internal events that threaten entity objectives (strategic, operational and reporting, compliance, etc.).

We do not discuss the development of risk concepts and related activities to analyze, quantify, and assess risks in this report. However, it is important to note that risk management policies—primarily risk measurement (probability and impact), as well as risk appetite, tolerance, and acceptance levels—are fundamental in determining the prioritization of risk mitigation or control objectives.

RISK MITIGATION/CONTROL OBJECTIVES

The risk mitigation or control objectives (hereafter referred to as control objectives) of a given process must be defined strictly on the business and governance objectives. This must be done on a comprehensive basis to guarantee a balanced, consistent approach in the design of the internal controls.

The prioritization (or weighting) of a control objective can be based on the number of risks it is mitigating or the dimension/importance of those risks. Control objectives of a given process can apply

to any one of several sub-objectives of business or governance goals. Exhibit 2.1 shows examples of risk mitigation/control objectives, identifiable from broader entity goals.

Exhibit 2.1: Risk Mitigation and Control Objectives	
Business or Governance Objective	Examples of Control Objectives
Ensure quality of product or service	Respect time standards or ensure general timeliness of the activities.
	Ensure quality of product from production processes, per standards.
	Ensure the availability of the service and its business/operational continuity.
	Meet contractual standards for the service or product.
	Guarantee the proper identification and need of buyer/customer.
Ensure partnership/key supplier performance in support of business objectives	Ensure financial and legal viability of supplier.
	Ensure valid contractual obligations.
	Guarantee reliability of supplier performance.
	Ensure service level (qualitative or quantitative) in line with expectations/needs.
	Ensure optimize cost at required quality standards.
	Guarantee technological updates in line with market and legislative context.
Ensure resources necessary to support processes	Guarantee adequacy of skill base.
	Ensure alignment of quantity of adequate resources with requests.
	Ensure services received consistent with services requested.
	Achieve timely resource renewal/replacement to avoid business interruption.
Ensure full respect/compliance to laws and regulations	Ensure information use and access in conformity with standards to ensure respect of privacy.
	Ensure client identification for purposes of anti-money laundering regulations (financial sector).
	Ensure acquisition of proper client risk profile as the basis for marketing financial products (banking sector).
Safeguard assets	Ensure restricted access to ward against illicit acts by outsiders or employees.
	Protect physical assets from natural events.
	Ensure employee security.
Safeguard information	Ensure confidentiality of information.
	Guarantee information integrity.
	Guarantee accessibility and usability of information.

Exhibit 2.1: Risk Mitigation and Control Objectives (continued)

Business or Governance Objective	Examples of Control Objectives
Ensure reliable financial reporting	Ensure the substance of transactions backing the accounting entries.
	Guarantee completeness of accounting registrations.
	Guarantee accuracy of accounting entries (precision, ratification, valuation, classification).
	Ensure completeness and timeliness of financial information for management needs.
Ensure the reliability of management information, bases for decision making	Ensure the substance of the transactions backing the financial or management reporting information.
	Ensure the completeness of information reported to customers, management reporting, and financial reporting.
	Ensure the accuracy of information reported to customers.
	Ensure the accuracy of information necessary for the operational process to be performed.

From the process objectives to the control objectives, one proceeds to their association to risks and to the actual controls in place. While macro-categories of such goals are fairly easy to identify at the entity and process level, the definition of an appropriate set of specific control objectives is the key to ensuring a complete analysis of risk coverage.

Exhibit 2.2 exemplifies this association. The risk weight is addressed later in relation to the methodology for assessing the overall internal control.

Exhibit 2.2: Risk Weight

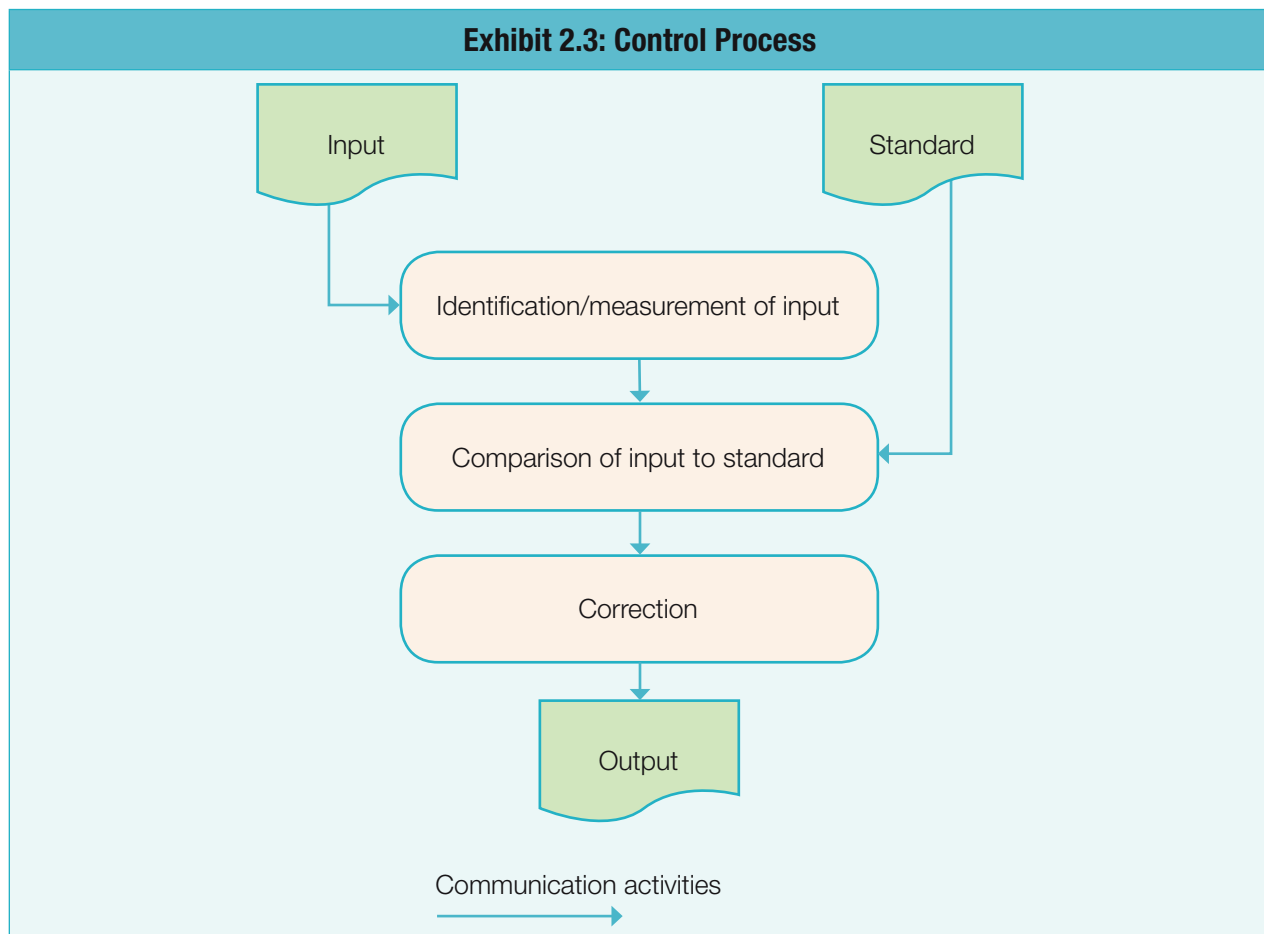
Business or Governance Objective	Risk	Risk Level ⁷	Control Objective	Example of Control
Maximize revenue from selling activity	Incorrect pricing for market conditions; loss of customers	5	Ensure product sale at the highest possible negotiated unit price	Periodic review of the adequacy of the pricing model for new and existing products
Ensure quality of product or service provided	Customer dissatisfaction for poor service or after sale assistance	3	Ensure that personnel are adequately trained and competent	Control of e-learning test results on certain aspects related to product knowledge
Ensure full respect of laws and regulations	Penalties arising from inadequate employee safety measures	4	Guarantee employee safety measures	Control by the supervisor of the access to work places using standard safety equipment

ATTRIBUTES AND CHARACTERISTICS OF INTERNAL CONTROLS

Based on the control objectives, controls in a multitude of forms basically perform in a three-step process:

- Identification or measurement of a certain existing situation (e.g., behavioral, informational, circumstantial, etc.), generically called *input*
- Identification of a deviation from a defined standard or a desired/expected outcome
- Activation of a corrective action to reach the desired outcome within a reasonable level

Thus, any control must be analyzed based on the desired outcome, whether it is represented by a standard or a more discretionary comparative point of reference (e.g., managerial, manual, automated, etc.). Exhibit 2.3 demonstrates the control process from input to output.



Each of these control steps or components must be considered in the overall assessment:

- Determining the standard or desired outcome and/or limits of acceptable exceptions

- Capturing the input (identifying the actual circumstances and how the information is collected)
- Ability to compare the input or the actual situation to the desired outcome or standard
- Type and timing of corrective actions in the case of a gap between standard and actual
- Information processes that support the communication of control results and guarantee the control process in terms of information (e.g., verbal, written, data processed, etc.)

Any control, whether simple or complex, manual or automated, can be analyzed based on the combination of these components.

COMPLEMENTARITY WITH THE COSO MODELS

The previously mentioned characteristics and objectives of control—risk based—are fully consistent with the models issued by COSO, both as to the internal control system (COSO I) and the enterprise risk management framework (ERM or COSO II).

CAM places emphasis on a comprehensive process of defining entity and process control objectives. This is fundamentally aligned with the objectives-setting process of ERM (as well as the necessary, practical application of the concepts of the COSO model governance objectives).

The assessment criteria of CAM captures all of the aspects contemplated in the component “Control Environment” of COSO I. The CAM methodology covers both control activities and monitoring controls foreseen by COSO. It is also fully applicable to the control processes relevant to HR (e.g., incentive systems, etc.).

The key to assessing the internal environment of ERM is the evaluation of pervasive entity processes, such as HR, strategic planning, and processes governing the allocation of resources. The evaluation of risk identification, assessment, and response are ERM processes that also fall fully under the scope of the CAM methodology. It completes the full assessment of the internal control systems within ERM.

ASSESSING RISK-BASED INTERNAL CONTROLS



When it comes to internal controls, effectiveness is determined based on two distinct areas:

- The architecture or design of the system (control attributes) that encompass the intrinsic characteristics of the process, as well as interrelationships with other processes
- The level of actual performance or functioning of the system, which may range from partial to full execution of the controls as they were designed to be performed

The overall assessment of an internal control system’s effectiveness is based on a combination of these conclusions.



Once the controls are identified across the process, in relation to control objectives, the first step is to understand the components. This will help you:

- Verify the completeness of the control
- Understand the relationships between the various control components

The next step is to assess the adequacy of each control with respect to the control objective(s). The aggregation of these analyses throughout the various activities of a process will allow the overall evaluation of the internal control system. However, the control analyses must be integrated with the necessary evaluation of the cost-benefit factors. This collection, integration, and evaluation should be completed for the key processes of the entire organization's internal control system.

The overall adequacy of internal controls is determined by:

- Effectiveness, which is the capacity to guarantee the minimization of the probability and impact of any risk event, within determined limits
- Cost-benefit factor, which is the capacity to guarantee that the overall cost of the control does not exceed the cost that will incur if the risk event takes place

Ample analysis can be conducted to seek maximum efficiency, which is intended as the optimal balance between the effectiveness and cost-benefit factors of the controls. In general, the greater the effectiveness of a control, the greater the cost; alternative control solutions can be deployed in search of a positive marginal benefit (possibility to improve the effectiveness/cost-benefit factor ratio).

OVERVIEW OF THE ASSESSMENT CRITERIA

The control objectives of a given process have differing degrees of importance. The level of importance is based on the significance and number of the related business and governance objectives. It is also measured in relation to the level of exposure to the related potential risks threatening their achievement.

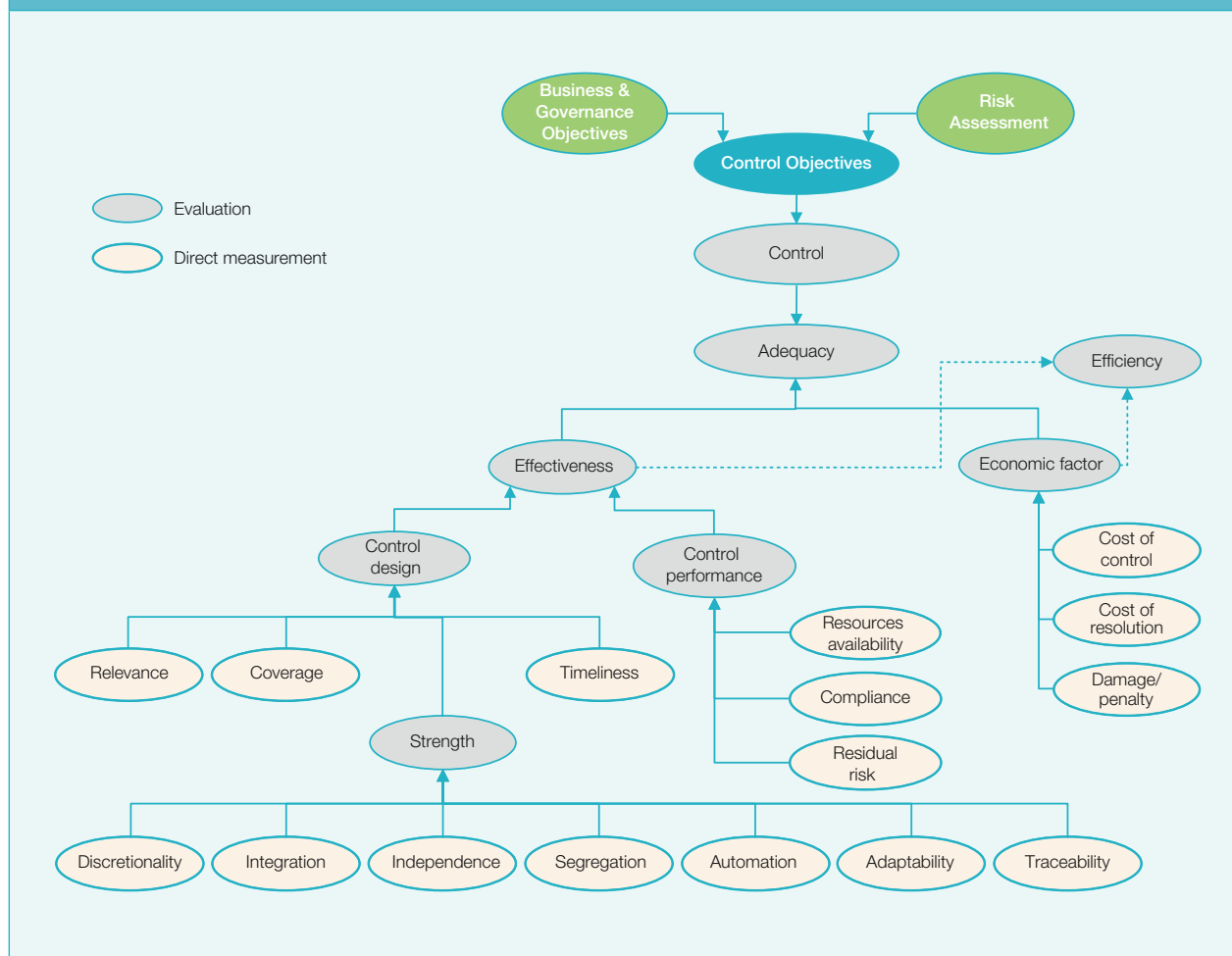
The model proposed here maximizes the objectivity of the internal control system's assessment.

The various criteria are measured based on a quali-quantitative scale that minimizes discretionary judgment of the analyst. It is based on elements that are objectively identifiable, both by the process owner and auditor.

This methodology fully satisfies the assurance objectives required by the audit committee. It does so through the predefined criteria and the relations between the control, the comparison to an expected outcome, the corrective remedies, and the objectivity foreseen in assessing the criteria.

The criteria of CAM is illustrated in exhibit 3.1.

Exhibit 3.1: Comprehensive Assessment Model (CAM)



CRITERIA TO ASSESS THE DESIGN OF INTERNAL CONTROLS

The evaluation of the adequacy of the architecture or design of the internal control system must be conducted process by process. It should consider the relevance of addressed control objectives and the attributes of the controls designed to achieve them.

As mentioned, the control objective is the fundamental base of analysis. For this reason, each control objective of the activity or process under analysis should undergo its own assessment. Such an approach may appear quite analytical at first; however, it will soon become clear that the benefits clearly outweigh the cost of thoroughness.

In addition to the pure reliability of the methodology, the primary advantage of this approach is the ability to make a true assertion of the adequacy of internal control. It does so in relation to a particular business objective and/or several associated governance objectives. This capability will satisfy the specific assurance needs of the board, audit committee or other governing bodies, and top management. For example:

- The assurance provided on processes underlying the financial reporting objectives will be of specific interest to the audit committee as well as the chief financial officer and can be relied upon by the external auditors in planning their work.
- The assurance provided in relation to product quality objectives intended to mitigate several risk events (customer dissatisfaction, legal, competition, etc.) will be of specific interest to the board, audit committee, executive committee, strategic planning head, and so on.

The following list summarizes the assessment criteria for the design of internal controls, and a complete explanation is presented afterwards.

- a. *Relevance*: the level to which the control activity addresses the pertinent control objective under analysis
- b. *Timeliness*: how long it takes for controls to respond to negative events. This element measures the ability to identify and correct a negative event, either by elimination or limiting its impact on the control objectives. Measurement is based on evaluating the control's responsiveness within a given time frame. This measures the moment the negative event occurs and the time that the actual effects or consequences arise, as a result.
- c. *Strength*: the strength of a control is determined by a series of factors that influence the probability of control effectiveness should related risks arise
 - c.1 *Discretion*: the level to which the control is discretionary or subjective, that is, if it is based on strict standards versus human judgment (who, what, and how the control is performed)
 - c.2 *Segregation*: the level of control segregation that goes beyond the well-known concept of separation of roles and duties between process activities, which are typically focused on conflicts of interest promoting fraud. At this level, it measures the degree of segregation found between the subjects responsible for the different phases of the control itself (see exhibit 2.3) to ensure the identification, diagnosis, and correction of any exceptions (errors, irregularities, structural failures, etc.).
 - c.3 *Independence*: the independence element measures the capability of the control owner to manage resources (technical, human, informational, economic) so that the control is most effective, acquiring or integrating resources as needed
 - c.4 *Integrative control factor (integration)*: the degree and manner in which the control reinforces other control processes for the same objective
 - c.5 *Automation*: the degree to which control process are activated by automated systems (information systems, mechanical devices) that reduce errors derived from human behavior

- c.6 *Adaptability*: how adaptable the control is to fluctuating volumes of activity (i.e., if the control is susceptible to the volatility of the controlled activities, it is less effective)
- c.7 *Traceability*: how traceable the control is, which allows it to be verified subsequently in all respects
- d. *Coverage*: the level in which all significant risks are addressed. In other words, the level of coverage of multiple control objectives, which in turn are based on the business and governance objectives of the process and related risks.

Relevance

Relevance measures the level to which the internal control process, in all its essential steps, addresses the specific control objective under analysis. Relevance can be interpreted as:

- The capacity of controls to fully or partially intercept negative events, given specific means to identify and diagnose them
- The ability to reduce exceptions to acceptable levels through specific corrective actions without interfering with regular operations

For example, exhibit 3.2 provides an illustrative evaluation table to maximize objectivity in the evaluation process.

Exhibit 3.2: Assessment of Internal Control	
Assessment of Internal Control for Level of Relevance to Control Objectives ⁸	
Rating 1	The full control process (identification, measurement, standard setting, and correction) is designed to address the specific control objective.
Rating 2	Either the identification/measurement process <i>or</i> the standard setting has not been designed to address the specific control objective.
Rating 3	While the identification/measurement process and the standard-setting process has been intended to address the specific control objective, the correction process has not.
Rating 4	Either the identification/measurement process <i>or</i> the standard setting has not been intended to address the specific control objective as well as the correction process.
Rating 5	The entire control process does not address the control objective (identification, measurement, standard setting, and correction).

A practical case study applying this table is illustrated in exhibit 3.3.

Exhibit 3.3: Internal Control Case Study	
Internal control	Ensure census/recording of existing customer base in marketing database.
Control objective	Guarantee the completeness and accuracy of the customer database for marketing activities.
Description	The employee of the sales office verifies at the moment of a new contract that all data regarding the customer has been correctly recorded in the system (address, name, postal code, ID number). In the case of exceptions, query is made to the accounting department.
Assessment of the control criteria of relevance	Rating 5
	Performance of the information check is limited to the moment of contract stipulation. It does not capture variations in the client data without new sales activity. The standard does not predefine aspects such as address (legal headquarters, shipping address, etc.) for the future marketing campaigns, nor does it establish the means for checking the address. The response to exceptions does not necessarily ensure the resolution of the problem.

Strength

The strength of an internal control is based on several criteria. Each requires an independent evaluation and contributes to an overall evaluation of the robustness or strength of the control. An example of the overall assessment process of the strength criteria is illustrated later in this report.

The following list contains the seven factors that contribute to the evaluation of strength.

Discretion Factor

The level in which a control is nondiscretionary is the extent that control activities are predefined and objective. There are several areas where specific predefined rules can be defined:

- When should the control be activated?
- What should be subject to control (activity, data, documents, etc.)?
- How is the control performed; in particular, with respect to what standard or with what tools or resources (e.g., information system)?
- What specific corrective actions are foreseen and how are the control activities documented?
- Who performs the control?
- When is the control activated (what is the deadline, frequency, circumstance)?

A nondiscretionary control activity must not be confused with the mere existence of procedures or policies. Their existence does not guarantee that they actually describe the aforementioned information.

In certain situations, control systems are considered to be highly predefined simply because there are few (or no) alternative ways that they can be performed. This can occur in a noncomplex environment,

with a single accounting unit or a single information system, or in a production area where control must be completed in a single, physical environment.

The level of discretion can also depend partially on the management level accountable for the control. For example, high-level management controls are frequently discretionary in nature, in that the standard or the types of response are based on subjective management decisions and judgment.

This can be quite acceptable in the case of nonrecurring circumstances. However, it should be considered a weakness when the risk is recurring and frequent.

In the area of line controls, a high degree of discretion applied within control activities demonstrates a significant weakness, especially when segregation of the control processes is low. Exhibit 3.4 shows an example of an evaluation table for the level of discretion.

Exhibit 3.4: Level of Discretion	
Assessment of Internal Control for Level of Discretion	
Rating 1	The control standard and response time are strictly defined and the individuals who are accountable for the control are clearly established.
Rating 2	The control standard and response time are strictly defined and the department/unit/group of individuals accountable for the control is established.
Rating 3	The control standard and response time are discretionary, but the individuals accountable for the control are predefined.
Rating 4	The control standard and response time are discretionary and the department/unit/group of individuals for the control are predefined.
Rating 5	The control standard and response time are discretionary and the individuals accountable for the control are not predefined.

Exhibit 3.5 provides an illustrative application of this evaluation table.

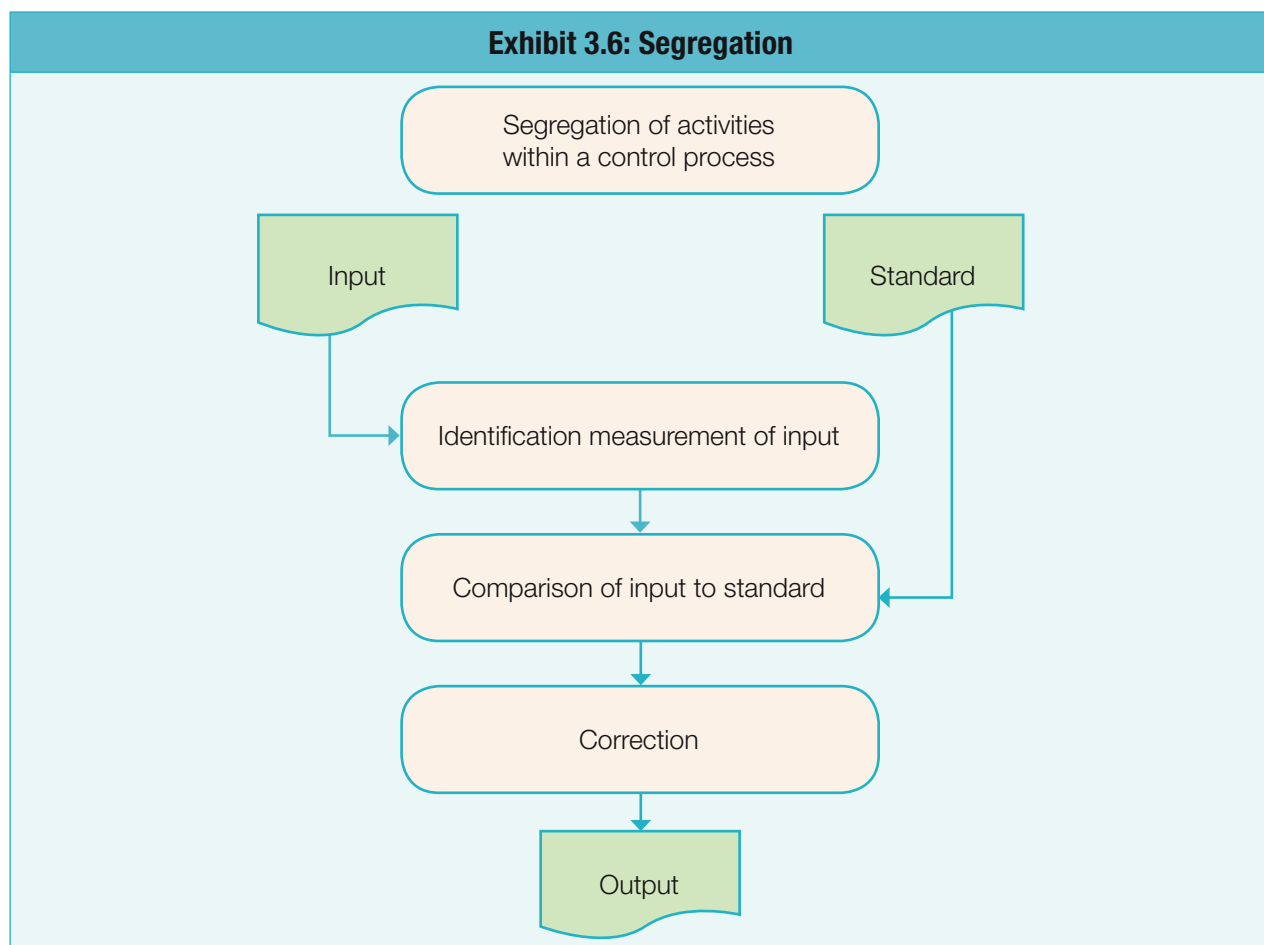
Exhibit 3.5: Discretion Example	
Internal control	Correct payment of receivables after due date is verified.
Control objective	Ensure financial coverage for all services is provided to customers.
Description	The employee accountable for administrative credit control verifies that the customers, automatically solicited for payment, have transmitted amounts due. In absence of payment, the employee prepares and sends a second solicit.
Assessment of the control criteria of discretion	Rating: 4
	The standard does not define the following aspects: when the control should take place, which systems or documents should serve as reference for the identification of the payment. The response time (for example, one week after solicit) is also not predefined. Instead, the standard does define the accountable person and the corrective action.

Segregation

Segregation is traditionally referred to as the separation of operational activities from control activities to ensure that exceptions or irregularities are actually captured. For this reason, it is typically related to organizational aspects of attributing responsibility, which avoid conflicts of interest.

In this model, the segregation element assumes a broader sense. The more the activities within the control process are separated, the stronger the control to prevent malfunctions of the control process itself, not necessarily determined by conflicts of interest. For example, a separate responsibility could be attributed to the person/function that establishes the standard of control (e.g., a quality department establishes a predefined quality standard that the operational control function uses in conducting its controls).

If the standard of reference for the control process is designed by the same person who performs the control itself, the risk of that control functioning incorrectly is greater. This risk can manifest itself in the creation of a standard that is inappropriate, rendering the control ineffective by not capturing the true anomalies of the operations. Exhibit 3.6 maps the segregation of activities within a control process.



Another example, a lack of reaction in the correction phase, would be identified if a segregated function monitors the activity. An interruption in the measurement process would be caught by a separate unit responsible for the comparison of operations to standards and/or correction.

Segregation can be obtained with:

- A separate person or function that gathers the relevant information to be controlled. This may include IT processes that are separately defined/elaborated from the controlling function.
- Separate responsibility for the correction process from the control process
- Separate responsibility for the communication of results

This is not to say that all phases of a control process must be segregated; it is simply to say that the greater the segregation, the greater the degree of strength in assessing the control. However, if the control objective is related to fraud prevention, then high levels of segregation should most likely be present.

Cost-benefit factors are relevant here, as segregation implicates higher cost for the control. Cost-effectiveness requires saturation of resources used in the various control activities, while a high-probability impact scale of the risk may justify the cost. Exhibit 3.7 provides an example of an assessment table for segregation criteria.

Exhibit 3.7: Level of Segregation

Assessment of Internal Control for Level of Segregation	
Rating 1	Those who are accountable for the control are different from those who perform the related operational activity. All elements of the control process (input, standard, collection, comparison, and correction) are performed, or provided for, by different subjects or systems of different groups/units/departments.
Rating 2	Those who are accountable for the control are different from those who perform the related operational activity. Some elements of the control process (input, standard, collection, comparison, and correction) are performed, or provided for, by different subjects or systems.
Rating 3	Those who are accountable for the control are different from those who perform the related operational activity. All elements of the control process (input, standard, collection, comparison, and correction) are performed or provided for by different subjects/systems within the same group/unit/department.
Rating 4	Those who are accountable for the control are different from those who perform the related operational activity. All elements of the control process (input, standard, collection, comparison, and correction) are performed or provided for by the same subject.
Rating 5	Those who are accountable for the control are the same as those who perform the related operational activity for all elements of the control process (input, standard, collection, comparison, and correction).

Exhibit 3.8 demonstrates an application of the control criteria of segregation.

Exhibit 3.8: Segregation Example	
Internal control	Control to ensure that the purchasing request relates exclusively to the requirements or resources needed.
Control objective	Ensure fair access to bidding to all eligible suppliers.
Description	The purchasing department checks that the purchase requisition does not contain restrictions as to the supplier nor indications that restrict or exclude the selection of certain companies included in the approved supplier list (which is defined by the supply strategy committee, headed by the legal affairs). Should this be the case, the requisition is rejected and sent back.
Assessment of the control criteria of segregation	Rating 2 Those accountable for the control (purchasing department) are different from those responsible for operations (department providing the request for purchase). Part of the standard (approved supplier list) is defined by a subject outside the purchasing department.

Independence

This element measures the degree to which the owner of the control is independent with regard to the management of resources necessary for the execution of the control itself:

- *Informational*: not dependent on information from sources outside the area to exercise the control activity
- *Human*: increasing or decreasing resources, as needed, for control
- *Financial*: accessing monetary resources, as needed, for control
- *Technical*: able to access or adapt technology and technical resources, as needed

If the owner of the control is not in a position to readily access such resources, the control may be compromised. It may also be compromised if part of the control must be performed by acquired resources, such as outsourcing, and financial resources are limited.

The independence element regards both qualitative (competencies, culture, capability) and quantitative factors (number, amounts). Thus, the independence element measures the capability of the process owner of the control to manage resources so that the control itself is most effective. This includes the acquisition or integration of resources, as needed. This may be associated with the managerial level to which the control is attributed, as well as the organizational structure of the organization.

It is important to understand the difference between independence and adaptability, which will be illustrated later. Independence refers to the level to which one can guarantee the availability of resources to execute control activities. Adaptability refers to the degree to which the control is able to take into account changes in the risk environment surrounding the control. Exhibit 3.9 provides an example of the assessment of independence.

Exhibit 3.9: Level of Independence

Assessment of Internal Control for Level of Independence	
Rating 1	Independence of control with respect to means and timing of obtaining the necessary resources for the control.
Rating 2	Independence of control with respect to means <i>or</i> timing of obtaining the necessary resources for the control.
Rating 3	Dependency on either means or timing for the periodic establishment of necessary resources (human, technical, financial).
Rating 4	Dependency on both means and timing for the periodic establishment of necessary resources (human, technical, financial).
Rating 5	Continuous dependency on both means and timing for the establishment of necessary resources (human, technical, financial).

Exhibit 3.10 demonstrates an application of the control criteria of independence.

Exhibit 3.10: Independence Example

Internal control	Automated control of waiting time at the customer counter of the bank.
Control objective	Ensure respect of standard for maximum waiting time in relation to quality customer service. Guarantee meeting expected customer service levels (including communication of waiting time).
Description	The bank branch manager checks on a daily basis the status of waiting times for each operation of the service windows, the number of persons in line, and the number of counters open. On the basis of predefined time standards, (maximum 10 minutes) and the existing lines, the manager may decide to open additional service windows, requesting back office personnel to service clientele.
Assessment of the control criteria of independence	Rating 1 The branch manager autonomously monitors the risk of excessive waits by customers and can procure resources from back office activities to compensate when needed. If the manager performed the control on the basis of a machine that calculates waiting time, or is required to ask the human resources department for additional manpower, the rating would be 3; this is due to the dependence of the control on other tools or departments.

Integrative Control Factor

The integrative control factor (also called integration criteria) measures the capability of the control in relation to a given control objective to reinforce and integrate, in a synergic manner, other controls contributing to the overall level of effectiveness of the internal control system. In an ideal system, a single control would be sufficient to preside over a given activity to reach the desired outcome.

However, this theory fails in complex situations where 1) there are many people involved, 2) there are relatively complex organizational structures, or 3) it is impossible to ensure complete segregation of first-level controls at a cost-beneficial level.

In such cases, it is necessary to introduce multiple controls that work in conjunction with themselves. These integrative controls may be performed:

- Consecutively, in conjunction with the initial control, through a second line control, an audit verification, or a monitoring function
- In parallel, often by some form of repetition of the control in a segregated area and/or by different individuals or means (i.e., using summarized data versus an analytical report, sample testing, etc.)

The consecutive type of integrative control is particularly useful when line controls are delegated to a wide number of people or organizational units, or characterized by a high level of decentralization. When this control represents a broader monitoring process, it may lose some relevance to the specific control objective, but it still contributes to reinforcing the achievement of the control objective.

For an example of this, consider the verification of an authorizing signature by a separate department. This confirmation can ascertain that the control is appropriately authorized, though it is not necessarily able to discern the validity of the underlying transactions.

Parallel controls, instead, are intended to directly mitigate risks related to the same control objectives of the first control. Partial duplication of the control reduces the risk of not achieving the control objective but increases the cost of the control. Exhibit 3.11 illustrates an assessment table for evaluating the integrative element of control.

Exhibit 3.11: Integrative Control Factors	
Assessment of Integrative Control Factors	
Rating 1	The second-level control fully checks the initial control for complete and correct execution, including exception management (full duplication).
Rating 2	The second-level control checks the initial control for complete execution, as required, and tests on a sample basis the correct management of exceptions.
Rating 3	The second-level control checks the initial control both for execution and identification and treatment of exceptions on a sample basis.
Rating 4	The second-level control re-verifies only the identified exceptions.
Rating 5	The second-level control monitors general trends in identified exceptions.

Exhibit 3.12 demonstrates an application of the criteria regarding integrative control factors.

Exhibit 3.12: Integrative Control Example	
First-level control	An automated control on the quality of packaging of products, on a sample basis, check on presence and resistance of packaging, adhesive closure, labeling, inclusion of warning labels regarding toxic ingredients; tests on actual toxic level are made on the basis of a sampling process applying established statistical confidence levels.
Control objective	Ensures the quality of product (semi-finished, finished) in relation to defined quality standards in the various manufacturing phases.
Description of second-level control	The operators of the quality department, in the case that packages <i>do not pass</i> the first-level control, test the toxic content of the item and verify that the product does not exceed established limits. The samples are retained and the data is used to update statistics and quality standards.
Assessment of the criteria regarding integrative control factors	Rating 4
	The second control verifies toxic level only in packages already identified as at risk from the first automated control.

Automation

Automation is the control assessment criteria that measures the use of automated means and IT to execute the control process. Its complement is the dependence on the human factor to perform internal controls.

Automation allows for errors or anomalies that are typical of the human factor to be eliminated. The assessment must consider, however, the strength of the architecture and maintenance of the automated processes. In other words, controls for automated systems and IT represent a strong mitigation of the risk of error, on the condition that the overall management of technical and IT resources (i.e., planning, development, maintenance, launch, and operations) is free of systemic defects.

This control element includes both hardware and software. Therefore, it is not limited to databases that may support the communication processes of the control.

Should a low level of automation be present, it is still possible to mitigate risk through adequate controls within HR management (e.g., processes for training, incentives systems, disciplinary systems, control culture).

Finally, obtaining a high rating of assessment for this criteria may not be possible in relation to cost-benefit issues, which will not necessarily allow for the standardization and automation of the control process. Exhibit 3.13 provides an example of an assessment table for evaluating the automation element of control.

Exhibit 3.13: Level of Automation	
Assessment of Internal Control for Level of Automation	
Rating 1	All elements of the control process (delivery of information [input], measurement, standard, comparison, and correction) are supported by automated systems or IT.
Rating 2	The control process with regard to input, measurement, and comparison is supported by automated systems or IT.
Rating 3	The control process with regard to information collection and comparison is supported by automated systems or IT.
Rating 4	The control process only with regard to information collection is supported by automated systems or IT.
Rating 5	No phase of the control process is supported by automated systems or IT.

Exhibit 3.14 demonstrates an application of the control criteria of automation.

Exhibit 3.14: Automation Example	
Internal control	Control of accuracy of the PIN security code on a debit or credit card.
Control objective	Safeguard against unauthorized transactions and fraud.
Description	The security procedure of the ATM performs an automatic check on the consistency of the data with respect to master data (card number, expiration, PIN, validity, etc.). In case of exception after three attempts, the transaction is blocked and the card is withheld.
Assessment of the control criteria of automation	Rating 1
	All elements of the control process (input, measurement, standard, comparison, and correction) are supported by automated ATM system.

Adaptability

The adaptability criteria of control strength measures the ability of the control process to adapt to fluctuations in volume or any volatility of the underlying operations. This does not relate to changes in business or governance objectives (affecting, in turn, the control objectives) or other structural changes to the control environment or design. The control is measured rather for its ability to handle peaks and changes in the related operations that may or may not be programmed or predictable (e.g., seasonal versus business fluctuations).

The adaptability criteria of a control considers:

- Overall minimum and maximum time for execution of the control (see also the criteria *timeliness*)
- Volume of transactions or operations in a given period and types of associated risks
- Average levels of exceptions handled
- Quantity or resources foreseen (in the case of HR, this can translate to *full-time equivalent* executing the control process)

The adaptability element can affect the control directly by not allowing the control to form correctly. It can also affect the control indirectly by altering its timeliness (e.g., back logs, etc.). Diagnostic tools can be deployed to measure this criteria (e.g., measurement of variability of volumes, frequency of fluctuations, etc.), depending on the critical nature of the underlying operational risk.

Legal issues that place time constraints on controls and resources can limit the strength of adaptability. Exhibit 3.15 provides an exemplary assessment table for this criteria.

Exhibit 3.15: Level of Adaptability	
Assessment of Internal Control for Level of Adaptability	
Rating 1	The control process is able to manage volumes in excess of average without impacting negatively on the standard execution times.
Rating 2	The control process is able to manage volumes in excess of average with limited negative impact on the standard execution times.
Rating 3	The control process is able to manage average volumes at standard execution times.
Rating 4	The control process is able to manage average volumes with some risk of timing in excess of the standard.
Rating 5	The control process is able to manage volumes below the average.

Exhibit 3.16 demonstrates an application of the control criteria of adaptability.

Exhibit 3.16: Adaptability Example	
Internal control	Expenditure control
Control objective	Ensure that personnel costs are paid only for appropriate corporate expenditures.
Description	<p>The personnel office, at each monthly accounting closing, verifies every expenditure report against attached supporting documents. In the case of exceptions (lack of support, irregular documentation), the office refuses authorization of payment.</p> <p>The verification should require three minutes on average. A further minute is added to the standard in the case of rejection in order to complete communications.</p> <p>Historical statistics evidences that expenditure notes number on an annual basis from 1,500 to 3,200 requests.</p> <p>The number of rejected expenditure notes average at 33 per year.</p> <p>Time available by the one employee responsible for this control is no more than 14 hours per month. Should time required exceed this, the employee reduces the time allocation to the separate area of monthly closing of accounts.</p>
Assessment of the control criteria of adaptability	Rating 3
	<p>The control process is able to manage average volumes within the standard time.</p> <p>While if the maximum volume is reached, resources are not available to manage it, considering the normal level of exceptions experienced; the additional time required does not negatively impact the accounting close.</p>

Traceability

Traceability is the degree to which the internal control system is able to verify the internal control subsequent to its execution. This typically entails the availability of supporting documentation or formalized verifiable actions.

The assessment can be affected by legal requisites. For example, formal authorizations may be mandatory, data conservation may be specified legally, and type and timing of documentation may be predefined to allow for outside inspection.

A time element is introduced in the assessment by considering how long the documentation is available. Some controls, however, may need to be traceable only up to the end of the underlying operational cycle (e.g., production through to shipment).

When the risk of untimely correction is significant, the time limit for traceability may increase in relation to the need for integrating controls. Exhibit 3.17 provides an assessment table for evaluating the traceability element of control.

Exhibit 3.17: Level of Traceability	
Assessment of Internal Control for Level of Traceability	
Rating 1	The manner in which the control process (input, measurement, standard, comparison, and correction) is managed allows for a subsequent check or re-performance even well after the operational cycle has been completed.
Rating 2	The manner in which the control process is managed allows a subsequent check or re-performance within a certain operational period.
Rating 3	The manner in which the control process is managed allows a partial subsequent check or re-performance within a certain operational period.
Rating 4	The manner in which the control process is managed allows a subsequent check or re-performance only partially and/or in a very limited time frame.
Rating 5	The manner in which the information (input, standard, comparison, correction) of the control process is managed does not allow a subsequent check or re-performance.

Exhibit 3.18 demonstrates an application of the control criteria of traceability.

Exhibit 3.18: Traceability Example	
Internal control	Control of availability of funds in banking account to execute all requested transactions.
Control objective	Ensure transactions meet predefined financial limits.
Description	The bank clerk interrogates the information system for fund availability of the client. In case of insufficient funds or credit, the transaction is refused. The system logs who accessed the system and when and is conserved for five years while banking records have a 10-year retention period.
Assessment of the control criteria of traceability	Rating 2 The control is fully traceable and verifiable through the system log, which traces the execution of the control performed by the specific clerk. However, the operational period allowing traceability (five-year retention of logs) is below the 10-year legal requirement for document traceability.

Timeliness

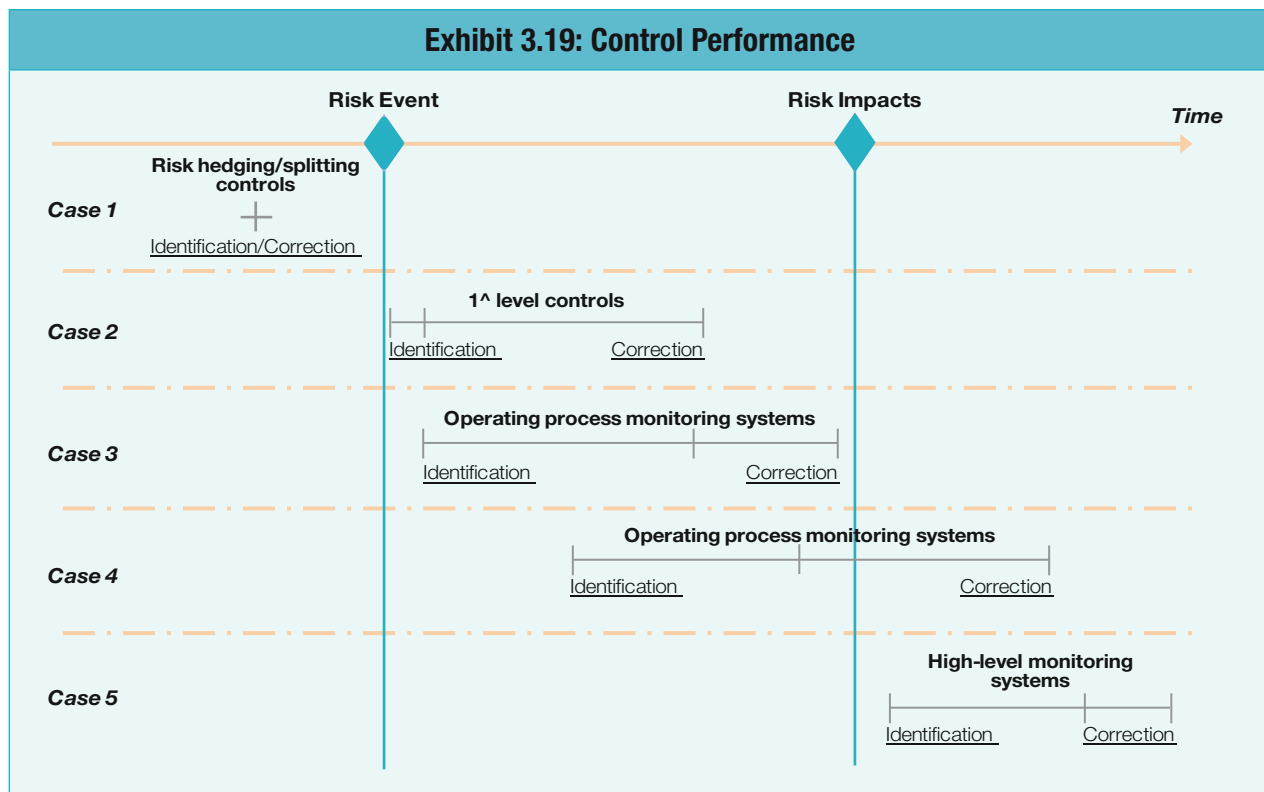
Timeliness is important when evaluating the adequacy of internal control. It measures the time to act or react in relation to:

- Collecting the control information and identifying exceptions or anomalies
- Activating the correction phase of a control activity to eliminate or reduce the impact of any exceptions or anomalies

Both types of response times must be analyzed based on the overall timing and nature of the risks that surround it, including the moment that:

- The critical event emerges
- The full risk impact actually takes place (e.g., losses, damages, penalties)

The combined analysis of all of the previous factors and considerations allows for defining specific assessment rating criteria. An illustration of control performance from risk event to risk impact is shown in exhibit 3.19.



The following cases demonstrate five time scenarios with identification of exceptions or anomalies, as well as their correction, with respect to the actual risk.

Case 1: The first case regards controls that prevent or reduce the risk (i.e., preventive controls, accounting provisions, insurance, and diversification) and actually limit the risk before it occurs or can have full impact. This type of timeliness is appropriate when the related risk is high and the time between the risk event and impact is short.

Case 2: The second case is typical of a line control that identifies the problem almost simultaneously to its occurrence. Here, the response is timely enough to prevent the full impact of the risk event. For example, interception of a defective lot during production with removal before shipping to the customer results in loss due to the expenses incurred. However, it does not result in customer dissatisfaction. In this scenario, careful attention must be paid to the timing of the correction, which may or may not be achievable before the loss impact, depending upon the operational environment.

Case 3: The third case is typical of monitoring systems over risks that, based on the speed of correction, are able to counteract the consequences of the risk event. They are particularly appropriate for control systems over risks that are recurrent and significant with a low acceptance level.

Case 4: The fourth case is related to operational monitoring systems covering risks that are not particularly frequent or significant. In this scenario, management accepts a certain amount of residual risk.

Case 5: The fifth case regards high-level monitoring systems that are typical of top management, which enacts strategic changes, reorganizations, and investments in response to significant emerging risks. These are integrative to lower-level operational controls.

Based on the previous scenarios, an exemplary tool for assessing the timeliness of a control response is shown in exhibit 3.20.

Exhibit 3.20: Level of Timeliness	
Assessment of Internal Control for Level of Timeliness	
Rating 1	Identification and correction of anomaly simultaneous to the risk event.
Rating 2	Identification of anomaly simultaneous to the risk event and correction within the time of full impact of the risk.
Rating 3	Identification of anomaly after the risk event and correction within the time of full impact of the risk.
Rating 4	Identification of anomaly after the risk event and correction after the time of full impact of the risk.
Rating 5	Identification of anomaly and correction after the time of full impact of the risk.

Exhibit 3.21 provides an illustrative application of the timeliness evaluation table.

Exhibit 3.21: Timeliness Example	
Internal control	Semiannual monitoring of actual sales by product in relation to sales plan.
Control objective	Ensure control over business objectives regarding sales volume or income.
Description	The head of the sales department checks twice a year that sales are in line with the plan using a detailed product line report. Based on this check, the next year's sales plan is adjusted.
Assessment of the control criteria of timeliness	Rating 5
	The identification of the risk event (lower sales than planned) is subsequent to the risk event itself and the correction takes place well after the impact (year after).

Coverage

Coverage does not have to do with the quality of the control; it represents the degree to which the control covers multiple control objectives and related risks. A control process can address operational control, reporting controls, security controls, etc. In fact, in an integrated and efficient control process, the design of controls is improved when it is structured to address all or several pertinent objectives.

Exhibit 3.22 demonstrates how coverage of control objectives is evaluated at overall process level, rather than single control level.

Exhibit 3.22: Level of Coverage	
Evaluation of Level of Coverage of Control Objectives	
Rating 1	81–100%
Rating 2	61–80%
Rating 3	41–60%
Rating 4	21–40%
Rating 5	0–20%

PERFORMANCE OR EFFECTIVE FUNCTIONING OF THE INTERNAL CONTROL SYSTEM

The evaluation of the performance or functioning of the system depends on:

- The availability of financial, technological, or HR needed to perform the controls
- Compliance to the controls as designed, assuming the controls are considered adequate
- The results of activities in place to monitor and measure possible residual risks; this ascertains the degree to which control objectives are not reached (i.e., related either to risk management policies or inadequate controls)

The results of evaluating the functionality of the internal control system determine the presence of residual risks above and beyond acceptable levels.

How the system's actual performance is evaluated is directly linked to the evaluation of its design. In fact, it is not possible to evaluate the true effectiveness of the internal control system's performance without assessing its design.

Thus, evaluating compliance of internal procedures and external regulation is only part of the internal control system performance assessment. Furthermore, compliance evaluation is only a fraction of the overall evaluation of the *adequacy* of the internal control system.

This principle challenges many preconceived notions on control. In addition, verification regarding the actual functioning of the internal control system is only possible when the design has been assessed and found to be adequate. If not, the verification process should regard the assessment of the impact of the residual risks resulting from a defective or inadequate system.

When internal audit verifies the effective performance/functioning of the system, the independence element of this function reinforces the global risk management and internal control system. However, this should not be confused with integrative control factors, such as second-level controls, which represent an integral part of the system itself.

Availability of Resources Needed to Perform the Controls

Sufficiency of resources necessary for adequate control (e.g., financial, technical, and HR) is required for an internal control system to perform as intended. This assessment is based on the assumption that the system has the appropriate allocation of resources to support all of its control elements.

Some of the control criteria are particularly sensitive to the appropriate availability of resources; for example, adaptability (the ability to adapt to fluctuating volumes) and timelines. If resources are inadequate, a positive evaluation of the conformity of the control system to the predefined procedures and norms will not compensate for the lack of resources. The compliance level is measured at a specific moment or time, while the adequacy of resources affects functionality over the long term.

As with the assessment of the design of the internal control system, specific criteria and assessment tables can be developed for control performance factors. Exhibit 3.23 provides a sample assessment table regarding the availability of resources for control.

Exhibit 3.23: Level of Availability	
Assessment of Internal Control for Level of Availability of Resources	
Rating 1	In the period considered, all resources (quantitative/qualitative) for the performance of the control were available for all levels of activity.
Rating 2	In the period considered, resources were sufficient for the performance of the control, including some activity above normal level.
Rating 3	In the period considered, resources were sufficient for the performance of the control for the activity within normal levels.
Rating 4	In the period considered, resources were not always sufficient for the performance of the control for the activity within normal levels.
Rating 5	In the period considered, resources were not sufficient for the performance of the control for the activity within normal levels.

Compliance

Verification of compliance foresees tests performed by a partially or fully independent body or function on a system that is sufficiently nondiscretionary and traceable. Independence is measured by the degree to which the controlling body is not involved in the management of the area or in making any decisions to change the system.

A monitoring body may perform compliance checks to enact adjustments to the system. This is perfectly acceptable from a management point of view, but it should not be construed as assurance over the control system provided by bodies such as internal audit. If the system is highly discretionary in the nature of its controls, it may be very difficult to verify its appropriate functioning, even if accountability is strong.

In some ways, the various phases of the control (e.g., input, comparison to standard, correction, etc.) can be too judgmental for an auditor or compliance officer to assess. Yet, in the same manner, if controls are not traceable, they may not be verifiable. Several factors can affect the traceability of information necessary to determine control compliance:

- The documentation produced after the control was not appropriately conserved
- The established time limits for retention of documentation have been exceeded
- Inability to access the information⁹

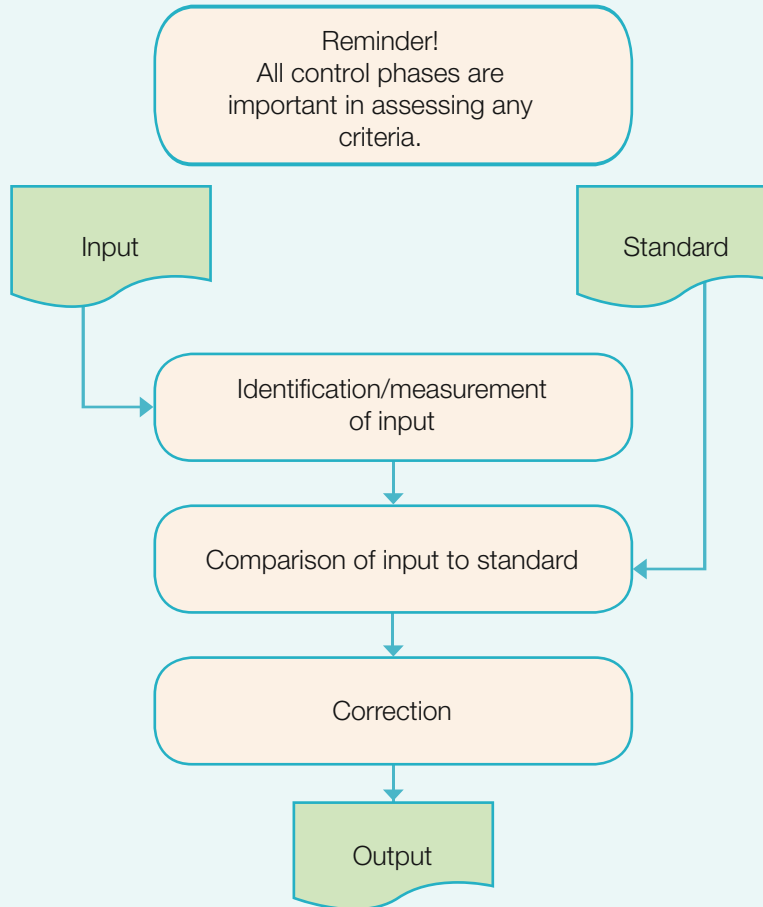
The significance of the compliance verification results depends upon the test methodology applied (sampling techniques, etc.). A test of conformity or compliance must be structured so that it fully verifies the control in all phases (e.g., input, comparison to the standard or expected result, correction). It must also verify the accountability of the control and the timing as established in the control system's design.

For example, an inventory manager must perform a monthly control on the reliability of inventory data for raw materials. Through comparison of data provided by the delivery documents and the quantities recorded in the inventory systems, the inventory manager obtains:

- The transport delivery receipts and the internal documents produced at the moment inventory is withdrawn for production. The inventory manager produces a sheet of totals (i.e., beginning balance, movements, ending balance), then signs and files it.
- The report of inventory produced by the accounting department and transmitted to the inventory manager by email.

After comparison, if there is a difference, the inventory manager informs the accounting department. Accounting will, in turn, correct the data and provide confirmation to the inventory manager. Exhibit 3.24 demonstrates the importance of all control phases in assessing criteria.

Exhibit 3.24: Assessing Criteria



Verification of this control asserts that it is effectively functioning and achieving the objective of providing reliable managerial data and physical inventory. The verification process requires testing of all six of the following criteria:

- The inventory manager's ability to receive documents (input) from the purchasing department, as well as dispatch documents from the production department
- Correct preparation of the summary sheet of inventory quantities, based on purchasing and dispatch data, and direct comparison to the accounting report
- The effective communication of differences by merchandise code
- The correction of the system records
- Consistency of the actual correction with the requested correction
- The appropriate and complete filing of documentation

It should be noted that the characteristics of this control are strong in terms of traceability and nondiscretion. This allows for effective compliance testing. Exhibit 3.25 provides an assessment table for level of compliance.

Exhibit 3.25: Level of Compliance

Assessment of Internal Control for Level of Compliance

Rating 1	The test demonstrated full conformity to predefined control procedures for the period examined.
Rating 2	The test demonstrated full conformity to predefined control procedures for the period examined, with some exceptions as to the manner or timing of performance.
Rating 3	The test demonstrated partial conformity to predefined control procedures for the period examined.
Rating 4	The test demonstrated partial conformity to predefined control procedures for the period examined, with exceptions as to the manner or timing of performance.
Rating 5	The test demonstrated low conformity to predefined control procedures for the period examined.

Measuring Residual Risks

This assessment criteria measures residual risks and ascertains the degree to which control objectives are not reached. This assessment process is typically performed by the audit activity and tests the actual impact of a lack of controls (residual risks).

This activity is applicable under different circumstances:

- When the design of the internal control system is defective, it replaces compliance controls, which are not applicable
- When the analysis of the system's design has not been fully completed and a full knowledge of the controls is not available
- When the design of the internal control system is available, but the cost of compliance testing is excessive

The fact that the internal control is insufficient/incomplete for risk mitigation implies that it is not possible to measure and manage risk events under continuous monitoring activities and ERM principles.

Low organizational maturity is implied by a pervasive need to apply techniques to identify residual risks arising from incomplete control design, rather than from conscious risk acceptance processes. At a higher maturity level, a process would be in place that periodically reviews the completeness of control design. The process would serve to capture, measure, and correct risk events, as well as the risk strategy applied. Such a process is also essential for updating applicable standards in the internal control system.

Residual risk testing is a one-time or occasional verification of events that directly or indirectly measure the risk impact. Following are two examples of residual risk testing.

Illustration 1

Consider the control objective of customer satisfaction in the context of a nonstandardized customer service process. In this process, significant risks are present for delays in service, errors in pricing, and inadequate ways to gather customer needs.

Assuming the extreme case, in which no internal controls are in place to ensure timeliness of customer service, residual risk testing would require finding a way to measure the level of effective

customer dissatisfaction. For example, the residual risk testing might include one or more of the following analyses: historical trend of complaints, average response time, invoicing patterns (reversals, etc.), frequency of cancelled contracts, or number/significance of legal disputes.

The residual risk measurement in this example consists of gauging certain negative events and correlating them to the associated risk of customer dissatisfaction. It can be performed by accessing and examining data available from the organization’s information systems.

This one-time exercise is clearly distinct from management control processes that would monitor operational performance systematically. Therefore, it should be cleared by management for purposes of obtaining an explicit acceptance of the residual risk emerging from the analysis. This may serve as a launching board for management to introduce more sophisticated risk management techniques.

Illustration 2

An adequate internal control system has been defined for the verification of prices applied to customers in the numerous sales points of an organization. Additionally, the sales function actively verifies the difference between standard sales prices and net sales cashed, with percentage limits. In this case, it would be possible to perform a compliance test on the line controls of all (or a sample) of the many sales points. Alternatively, the compliance test could apply to the monitoring activity performed centrally.

On the other hand, it may be more cost-beneficial to perform a test of residual risk. This could be done by analyzing the entire database for the average error rate in the application of prices, then comparing it to the acceptable error rate of the line or monitoring control. Exhibit 3.26 provides a sample residual risk assessment table.

Exhibit 3.26: Measuring Residual Risk	
Assessment of Internal Control for Measuring Residual Risk	
Rating 1	The test did not evidence residual risk.
Rating 2	The test evidenced residual risk within limits of acceptability and tolerance levels.
Rating 3	The test evidenced residual risk that exceeds the limits of acceptable risk but lies within related tolerance levels.
Rating 4	The test evidenced residual risk that exceeds the limits of acceptable risk and related tolerance levels.
Rating 5	The test evidenced residual risk that was not contemplated in the internal control system.

It should be noted that the residual risk measurement process can be used to provide *assurance* on the adequacy of the internal control system if acceptability and tolerance risk levels are defined. Without such parameters, residual risk measurement is still useful for establishing risk identifiers or *key risk indicators*. The internal control system grows stronger when these key risk indicators are transferred to the process owner, creating integrative control factors.

EVALUATION OF THE COST-BENEFIT FACTOR OF CONTROLS

In general, evaluation of the controls' cost-effectiveness should be subsequent to the assessment of the design and performance. Its main objective is to determine the reasonableness of the overall balance between effectiveness of controls and the cost of control.

The cost of control is measured based on fixed and nonfixed costs (e.g., dedicated resources, operational costs, costs of maintaining the information system, etc.) as well as external costs through partners of insurers. This cost should be compared to that of managing residual risk:

- Losses, damages or penalties, and/or lost income arising from risk events
- Cost of the resolution of risk events, which varies in relation to the actions needed to limit the impact of negative events that occur. These include internal costs to restore a situation (for example, reprocessing costs and advertisement investments to recover from reputational damage).

Illustration of Cost-Benefit Analysis of Internal Controls

A practical example is the case of an internal control system intended to provide a warning to the banking regulatory agency of all suspect financial transactions. In many countries, regulation anticipates penalties in the case of incomplete or incorrect information reported by financial institutions regarding financial transactions for clientele, which are later identified as related to illicit or illegal activity.

As the number of possible circumstances around irregular/illicit activity is infinite, the responsibility for identifying potential illicit activity falls on the financial institution, which is best positioned to create the means for intercepting it. This puts the financial institution in a situation where it is very difficult to eliminate all risks of incomplete identification, no matter what internal control system is in place.

The intention of the regulation is not to transfer the difficult job of surveillance of illicit activity from the authorities to the private entities, but rather to reduce the possibility that the entity can enhance profits without due consideration of its legality. Therefore, one of the purposes of the penalty, in a certain sense, is to nullify any opportunity for potential economic advantage from the client's passive conduct around illicit financial activity. This is a very good case study for evaluating and understanding the considerations around the balance of costs and benefits of an internal control system.

Full compliance consists of a system that identifies and immediately reports to authorities any transaction over legal limits. It should substantially reduce, if not eliminate, the risk of penalties for noncompliance.

Full compliance can also impact clientele. In some cases, clients must await authorization if their requested transaction exceeds legal limits and must be reported. Should controls exceed competitor systems, a certain level of business loss is possible.

Another extreme consequence of not putting an adequate internal control system in place, in terms of cost benefit, would lead to not only penalties but also potential loss of business. Current regulation allows authorities to halt business transactions.

Apart from these two extremes, there are numerous considerations around the evaluation of the costs and benefits of an internal control system. An incorrect or incomplete assessment will result in errors in risk management decision-making.

Following are examples of elements that can contribute to the assessment:

- Cost of *full-time equivalents* for HR efforts in the activities associated with the process:
 - Review and reporting performed by bank tellers
 - Review of transactions that are nonrecurrent, out of normal standards for reporting to authorities
 - Periodic updating of internal standards for reporting anomalies
 - Maintenance of related information systems
 - Training employees
 - Reviewing financial transactions, which are internally reported but should not be subject to reporting to the authorities
- Penalty costs for unreported transactions
- Commission income review on reported transactions

These aspects are affected by the internal control system's design based on:

- The predetermination of the standard, which may increase or decrease costs of capturing exception transactions
- The level of automation, which reduces the overall burden of HR and increases reliance on IT systems
- Level of integration of line controls, which impacts timeliness and completeness of reporting
- The level of systematic support processes (i.e., training of HR, IT development, updating of standards and procedures)

Analysis of cost-effectiveness may be necessarily limited when control objectives are associated with regulatory requirements. For example, it may be sufficient to conduct a general analysis of the overall cost of the control solutions.

When it appears that there is a significant imbalance, a more analytical approach is called to determine opportunities to replace controls with more cost-effective solutions. Exhibit 3.27 provides a sample assessment of internal control with regard to the cost-benefit factor.

Exhibit 3.27: Cost-Benefit Factor

Assessment of Internal Control with Regard to the Cost-Benefit Factor

Rating 1	The overall cost of the internal control system (identification, measurement, correction) is inferior to the potential losses derived from the risks, taking into account probability of occurrence.
Rating 2	The cost of the internal control system (with regard to identification and measurement) is inferior to the potential losses derived from the related risks, taking into account probability of loss; however, costs associated with the correction process can cause overall costs to exceed losses.
Rating 3	The cost of the internal control system in relation to measurement and correction exceeds the potential losses derived from the related risks, taking into account probability of loss.
Rating 4	The cost of the internal control system (identification, measurement, correction) exceeds the potential losses derived from the related risks, taking into account probability of loss.
Rating 5	The cost of the internal control system (with regard to identification and measurement) exceeds the potential losses derived from the related risks, taking into account probability of loss; however, costs associated with the correction process can cause overall costs to exceed losses.

CONTROL ASSESSMENT METHODOLOGY

The control assessment methodology provides a straightforward process for assessing individual internal controls. It uses appropriate rating systems designed for each of the criteria, as exemplified in the previous section. However, assessing a combination of controls is clearly more complex.

The correlation of a variety of control objectives, risks, and processes requires developing a rationale that ensures a balanced and objective control assessment, with due consideration to several business and governance objectives. Thus, any controls that respond to the needs of multiple control objectives are particularly important, as is the combination of controls contributing to a single objective. In addition, the controls that preside over the entity process of resource allocation (strategic planning, HR, etc.) will have a fundamental impact on the evaluation of the internal control system of many, if not all, other processes.

It is important to respect the following conditions, regardless of how simplified or complex the system of rules/criteria adopted:

- The assessment rules should be explicit.
- The assessment rules should be formulated with a top-down logic. At the top, there are general rules or principles that can be agreed upon at the board or audit committee level. More detailed rules follow thereafter.
- The application of the assessment rules is a bottom-up approach, with aggregation progressively reaching condensed information that is useful for presentation to top management and board members.

- The rules must be applied consistently and fully. If they are not initially sufficient to express an opinion, it is possible to integrate them over time.
- The application of the assessment rules must be documented to allow traceable evidence of the conclusions.

OBJECTIVE ASSESSMENT THROUGH QUANTITATIVE VS. QUALITATIVE APPROACH

The methodology in which the controls are identified and measured, in relation to the aforementioned criteria, is intended to provide an objective, nondiscretionary approach to assessing the internal control system of each process. This also allows a consistent bottom-up approach to combining process control evaluations to reach an entity-level assessment of the internal control system.

Control measurement can be:

- Quantitative, using quantitative variables by means of a systemic numerical scale. For example, the cost factor of control may be considered in terms of *full-time* equivalents occupied.
- Semi-qualitative, whereby ratings are based on a discrete scale and the classification is partially subjective/discretionary

ASSESSMENT METHODOLOGY FOR EACH INTERNAL CONTROL

The overall evaluation of a control is based on the combined assessment of the criteria presented in the previous section, using the predefined assessment rules. These rules consider a control attribute that is not based on a subjective (high, medium, low) rating scale, but rather on objective factors. Those factors can be observed—or identified and considered—in a given scale from positive to negative. Exhibit 4.1 shows a simple aggregation of assessment criteria for the evaluation of strength in internal control design.

Exhibit 4.1: Control Strength	
Exemplary Assessment of the Strength of a Control (Rating: 1 optimal - 5 poor)	
Criteria	Rating
Discretion	5
Integrative control factor (when applicable)	3
Independence	3
Segregation	3
Automation	3
Adaptability	5
Traceability	5
Strength (simple average)	3.8 (= Rating 4)

The defined criteria for strength are commonly shared for each control objective to which the control pertains. It is possible to enhance the rules for formulating an overall assessment of a control for a given objective while maintaining a predefined logical approach. In addition to considering simple and weighted averages of ratings, specific rules may be applied for certain criteria.

For example, in relation to the control objective of product quality, if the discretionary control factor rating is worse than *three*, it may be appropriate to maintain the overall assessment of the control at no better than *two*. Discretion contributes to the inherent weakness of the entire system.

There are corrective rules in an overall assessment approach that can be predetermined to construct an objective methodology. These rules allow for specific considerations and criteria to enter the evaluation process.

It is possible to introduce a *risk factor* to adjust overall assessment ratings to consider the underlying risk, and thus priority, of a given control objective. Thus, the rules for formulating an overall assessment of a control are based on a predefined, logical approach, which may consider average ratings as well as given criteria.

Some examples follow:

- If the control objective pertains to fraud prevention, the relative risk/priority is high (due to potential high regulatory or reputational impact), and the segregation control element is assessed at less than optimal (from *two* to *five*), the overall evaluation of the control design cannot be better than *three* (the same rule could apply to the traceability element).
- If the risk related to the control objective is low in probability and high in impact (e.g., disaster recovery) and the timeliness element of the control is assessed at anything worse than *one* (*two* to *five*), the overall evaluation of the control cannot be better than *four*.
- If the control objective and related risk pertains to ensuring reliable reporting, and the discretionary element is assessed at anywhere worse than *three* (*four* to *five*), the overall control evaluation cannot be better than *four* (the same rule could apply to the traceability element).
- This is related to the importance placed on the risk of manipulation as it pertains to accounting or reporting activities.
- If the level of the IT factor of the control is *one*, the overall evaluation of the control should be at least *three* or better (*one* to *three*), but it should not exceed the level of relevance.

Exhibit 4.2 provides an example of an evaluation of the design and performance of a control with respect to various control objectives, taking into account the underlying risk through predefined risk ratings. The guidelines noted provide the rationale in correcting the values to take into account the risk weights.

Exhibit 4.2: Assessment of Control

Exemplary Assessment of a Control (Rating: 1 optimal - 5 poor)

	Rules	Control objective 1 ensure service quality		Control objective 2 reliability of reporting		Control objective 3 ensure legal compliance		Overall evaluation
		Rating	Adjusted rating	Rating	Adjusted rating	Rating	Adjusted rating	
Assessment of design of control (rating 1-5, optimal to poor)								
Relevance		1	1	3	3	1	1	
Strength		2	2	2	2	2	1	
Timeliness	a	3	1.5	2	2	1	1	
Overall rating of design	b	2	1.5	2.3	3	1.3	1	1.8
Assessment of performance of control (rating 1-5, optimal to poor)								
Availability of resources		4	4	1	1	1	1	
Compliance	c	2	2	-	-	2	2	
Residual risk measuring	d	3	3	2	2	-	-	
Overall rating of performance			3		1.5		1.5	2.0
Overall rating of control	e		2.25		2.25		1.25	
Risk weight and overall assessment	f		3		2		1	2.1

Assessment Rules:

- Weighted half for control objective regarding quality; any assessment above *three* within the production area is considered higher in relation to the importance of this factor's contribution to the time-to-market control objective.
- Overall rating cannot be better than *three* if any element is rated worse than *two*; otherwise, a simple average is calculated.
- Compliance is not assessed and rated if the assessment of control design is rated worse than *two*.
- Residual risk measurement is not applied if design and compliance are rated better than *three*.
- Design and performance rating are given equal importance; thus, a simple average is calculated.

- Correction factor through risk weight. Higher risk and priority are applied through risk management techniques. They have been attributed to the quality objective in relation to potential reputational impact. Reporting reliability is considered higher risk in relation to pervasive reliance on information for decision-making purposes. Compliance, while considered essential, is also considered normal risk and priority. Overall evaluation is the sum of (risk weight x rating)/sum of risk weights.

It should be recalled that the assessment of coverage (of control objectives) is analyzed only at process or sub-process level.

EVALUATION OF THE INTERNAL CONTROL SYSTEM OF AN OVERALL BUSINESS PROCESS

Once the various controls have been individually assessed, it is now possible to combine results and consider the overall evaluation of the business process. By assessing the design of the internal control system of an entire process under this methodology, the auditor is able to express an opinion on the internal control system with maximum objectivity and diligence.

It also serves as advisory service to management, as its analytical nature can demonstrate effectively why and how residual risks are present, allowing management to consciously determine their acceptability. This evaluation phase allows for further weighting of control objectives and results based on risk analysis.

At the process level, the overall assessment of the internal control design is based on the quality of the controls identified within the process's phases, rather than the quantity. Moreover, the adequate controls illustrated:

- Relevance of each control in relation to the business and governance control objectives associated with the process
- Completeness of coverage of all associated control objectives
- Strength (consisting of its various critical elements)¹⁰
- Timeliness of the controls in responding to negative events
- Functioning of the controls
- A cost/benefit relationship of the controls

The assessment of the process is once again based on predefined rules. For example:

- If the evaluation of any of the primary factors of control (i.e., coverage, relevance, strength, or timeliness) is worse than *three*, the overall evaluation cannot be better than *three*.
- If the coverage of risk/control objectives is less than 80 percent, the overall evaluation cannot be better than *three*.
- If the risk relates to illicit acts/fraud and the segregation of the internal control system is worse than *two* (from *three* to *five*), the overall evaluation of the system's design cannot be better than *three* (from *three* to *five*).

First, it is necessary to assess the overall coverage of control objectives by the internal control system. This is one of the primary factors contributing to the strength of the overall system; however, it is examined and assessed only at process level.

Exhibit 4.3 provides an example of the overall evaluation of the internal control system of a single process, with reference to the various relevant control objectives. It demonstrates an exemplary assessment of coverage of control objectives.

Exhibit 4.3: Control Objectives						
Coverage of Control Objectives						
Process phase	Control	Rules	Control objective 1 ensure service quality	Control objective 2 reliability of reporting	Control objective 3 ensure legal compliance	Control objective 4 guarantee security
		a	Assessment of relevance (rating 1-5, high to nonexistent)			
A.1	Internal control 1		1	3	1	5
A.2	Internal control 3		2	5	5	5
A.2	Internal control 3		n/a	2	2	5
A.3	Internal control 4		n/a	5	3	5
A.4	Internal control 5		n/a	3	5	5
Overall relevance rating by control objective		b	1.5	3.6	3.2	5
Risk weighting of control objective			3	2	1	1
Overall assessment of coverage of control objectives		c	2.2			

Assessment Rules:

- A rating of *one* signifies that all phases of the control are relevant or pertinent to the control objective; *five* signifies that no area of the control was found pertinent, although the control was expected to be relevant to the objective.
- Certain control objectives are not applicable to the control and are marked by n/a (not applicable); overall assessment cannot be better than *two* if coverage of control objectives is rated worse than *one*. Otherwise, overall assessment is the simple average of the ratings.
- Sum of (risk weight x rating)/sum of risk weights; essentially three of the four control objectives are covered with high priority attributed to the quality control objective, resulting in an overall positive assessment.

Exhibit 4.4 demonstrates an exemplary assessment of the internal controls of the overall process.

Exhibit 4.4: Overall Process			
Assessment of Internal Controls of Overall Process			
Process Phase	Rules	Control	Assessment Rating
A.1		Internal control 1	2.1
A.2		Internal control 2	4.0
A.3		Internal control 3	1.5
A.4		Internal control 4	2.2
A.5		Internal control 5	3.5
Overall assessment of internal controls for entire process	a		2.7
Overall assessment of coverage	b		2.2
Overall assessment of cost-benefit factor	c		1
Overall assessment of internal control system of process			1.7 Rating 2

Assessment Rules:

- No weighting of subprocess contribution to overall system (e.g., business vs. support process) has been considered.
- See previous table.
- Not analyzed here.

EXPRESSING AN OPINION ON THE INTERNAL CONTROL SYSTEM OF A FULL PROCESS

CAM allows you to express a succinct and comprehensible opinion to the process owner and any other stakeholders. The predefinition of assessment criteria and methodology, as illustrated in the previous paragraphs, allows the assessor to manage all levels of complexity for formalizing reasoning and approach with appropriate rationale for any sharing or justification with third parties.

With experience, it is possible to further refine or develop the approach. It is also possible to allow for the integration of additional rules under unique or particular circumstances. An example of an overall scale for expressing an opinion is shown in exhibit 4.5.

Exhibit 4.5: Overall Process Assessment

Overall Assessment of the Internal Control System of a Process

Rating 1	Adequate or sound control system: a system that achieves the control objectives intended to mitigate the risks correlated to the business and governance objectives relevant to the process (based on risk acceptance strategy).
Rating 2	Adequate internal control system with some areas of improvement: a system that achieves the control objectives intended to mitigate the risks correlated to the business and governance objectives relevant to the process (based on risk acceptance strategy) with evidence of some areas, though not critical, subject to improvement to meet the requisites of sound controls.
Rating 3	Generally adequate internal control system, with some critical areas: the system achieves, in general terms, the control objectives intended to mitigate the risks correlated to the business and governance objectives relevant to the process (based on risk acceptance strategy). The characteristics of some of the controls, however, are not fully consistent with requisites of sound controls (for example, lack of automation, of traceability, of segregation, etc.).
Rating 4	Inadequate internal control system, subject to significant improvements: the controls only partially achieve the control objectives intended to mitigate the risks correlated to the business and governance objectives relevant to the process (based on risk acceptance strategy).
Rating 5	Insufficient internal control system: the combination of controls is not sufficient to achieve the control objectives intended to mitigate the risks correlated to the business and governance objectives relevant to the process (based on risk acceptance strategy).

Of course, once an opinion has been expressed, it does not mean that the evaluation process has ended. Changes in strategy, control objectives, legislative context, etc. can all change an assessment and the related status of the internal control soundness. Internal changes can also call for a reassessment: significant changes in accountability; significant IT system developments that alter the overall design of internal controls; emerging risks; and impacts of cost reduction measures on controls.

BUSINESS CASE

This section illustrates the comprehensive assessment of the internal control system design of a manufacturing company's business process. Fresco Company produces fresh milk products and considers product *quality* (its *business objective*) to be strategic to the organization's success.

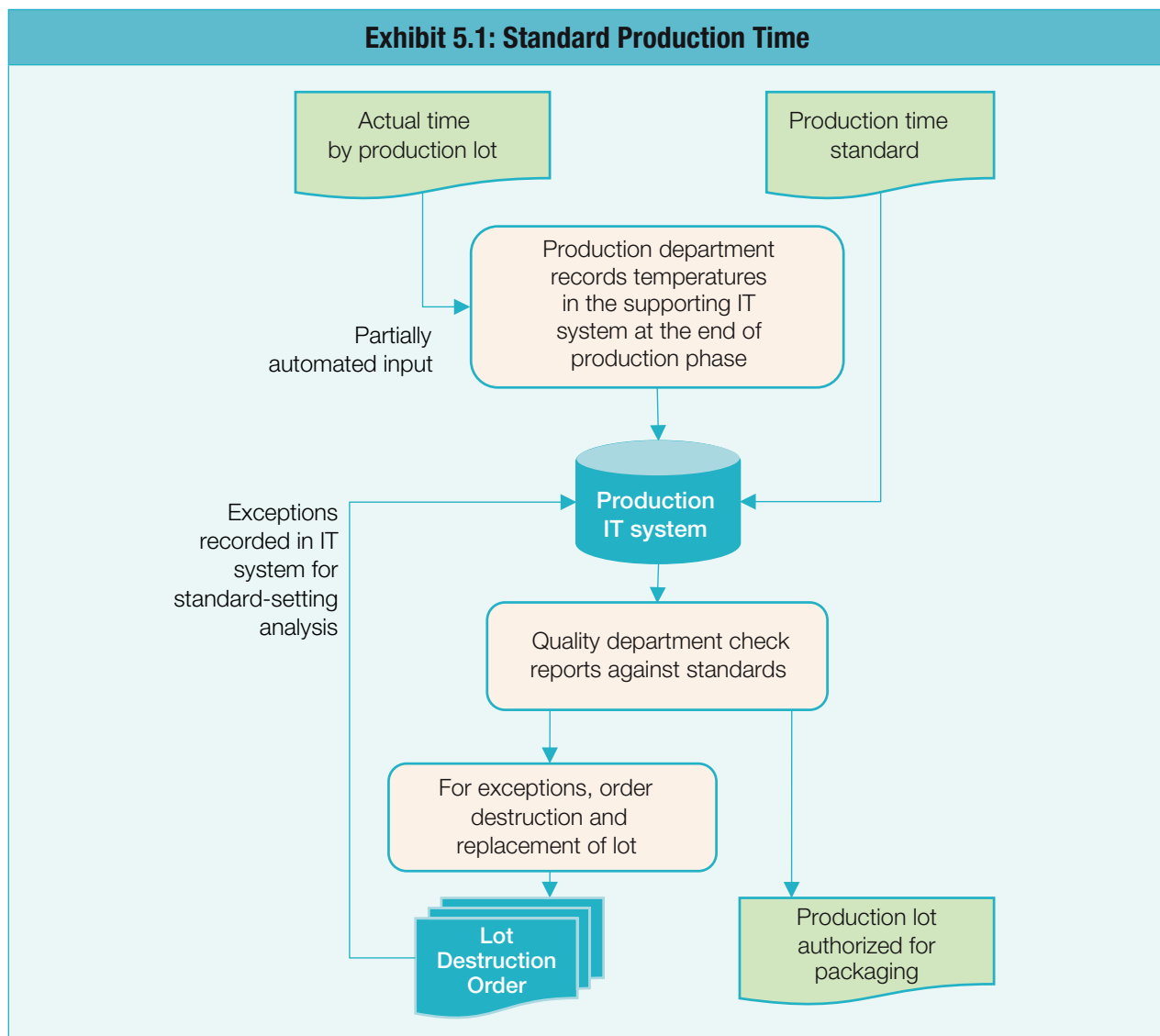
Quality is generally defined by preset standards and regards two *control objectives*:

- Ensure temperature standards for appropriate conservation
- Ensure achievement of time-to-market production standards

The process analysis reveals that an independent quality department is accountable for reviewing the production department's operating reports to verify that the actual time of each product production lot is within standard. If an exception arises, the quality department orders the production department to destroy and replace the lot.

The quality department is performing its check against quality standards based on reports that are, in part, automatically produced from the production department's operational systems. The other part is based on manual input by production workers.

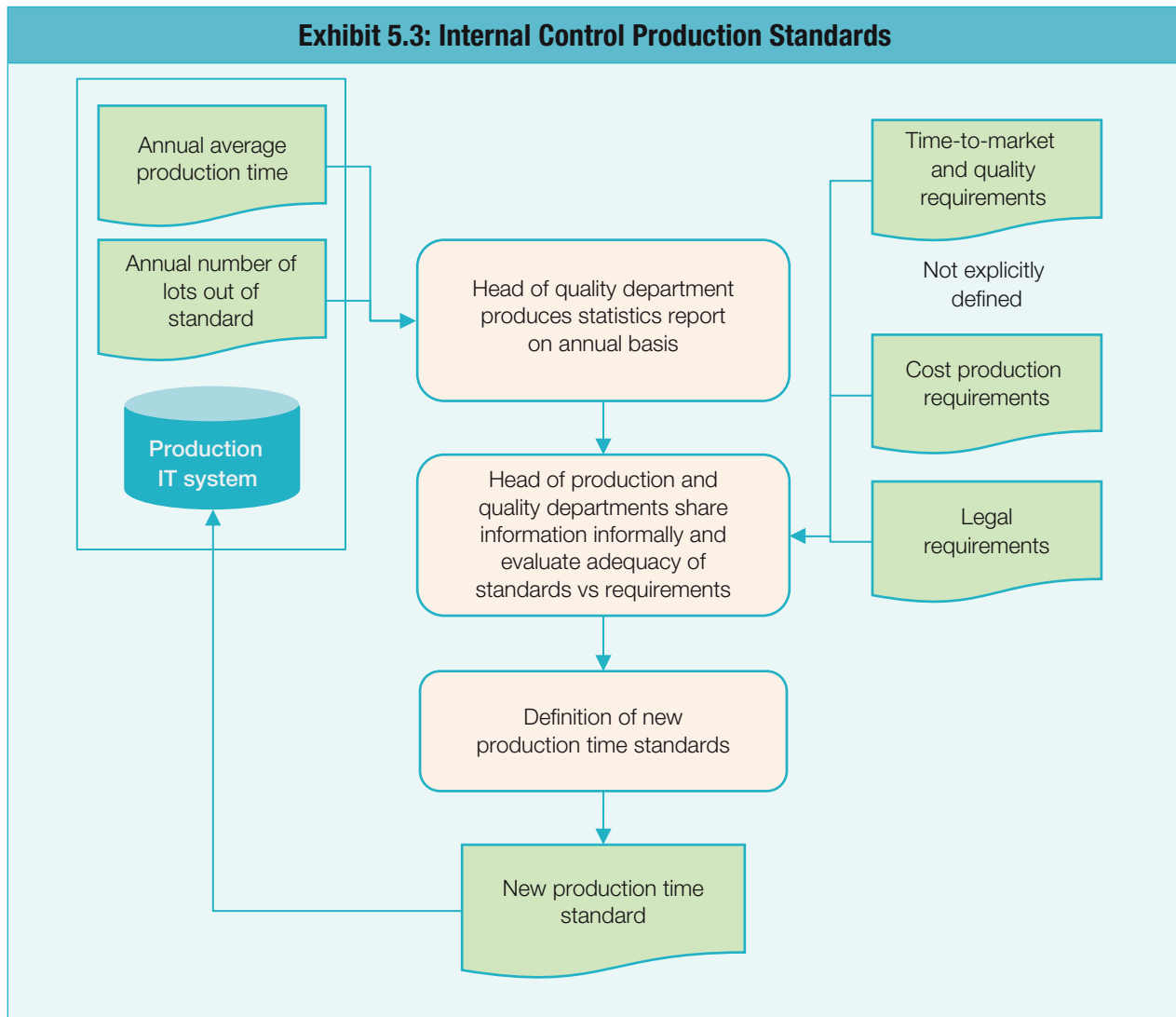
The quality standards are reviewed annually through statistical analyses. The review regards average actual production times and frequency of lots identified outside of quality standards. This allows for the systematic updating of internal procedures and standards. Exhibit 5.1 illustrates the control identified during the process analysis regarding the verification of standard production time.



Based on the comprehensive assessment criteria, this internal control is evaluated positively. The business objectives are met, ensuring time-to-market quality assurance and timeliness. The strength of the control is considered adequate in relation to the mix of control elements as shown in exhibit 5.2.

Exhibit 5.2: Control Production Time		
Assessment of control design: Control 1 - control of production time (Rating: 1 optimal - 5 poor)		
Criteria	Rating	Analysis
Discretion	2	The comparison between actual and expected production times is based on stringent nondiscretionary standards. However, the method and the frequency of periodic review by the quality function is not specified.
Integrative control factor	n/a	This control does not integrate other controls; therefore, not applicable.
Independence	4	The source of control information is the production department, which is not independent from the area subject to control.
Segregation	2	The quality department is accountable for the control, which is independent from the production department.
Automation	3	The data collection and reports analysis are partially automated, partially manual.
Adaptability	3	The resources dedicated to control do not change with modifications or peaks in volumes of production.
Traceability	3	The check performed is not fully traceable. Only the automated checks are documented.
Overall strength of control	2.8	<i>The overall evaluation of strength of the control is based, in this case, on the simple average of the individual criteria.</i>
Relevance	2	The control is specific to the control objective. However, the input phase and standard regard only production time and not the storage and shipment phase, which impact time-to-market objectives.
Timeliness	2	The control intercepts the exceptions immediately after production and prevents the lot from being shipped to the customer.
Assessment of overall design of control	2.3	<i>The overall evaluation of strength of the control is based, in this case, on the simple average of the individual criteria.</i>

A second control that emerges from the process analysis is updating the standards annually. Exhibit 5.3 demonstrates the flow between annual production time analysis and development of new production time standards.



The assessment of the control's strength is summarized in exhibit 5.4.

Exhibit 5.4: Internal Control Annual Review		
Assessment of control design: Internal control 2 - annual review of production time standards (1 optimal - 5 poor)		
Element	Rating	Analysis
Discretion	3	Only the requirements related to legislative norms are predefined. Discretion is exercised both for market requirements and production cost aspects.
Integrative control factor	n/a	Not applicable. Although this control relates to the same control objective of guaranteeing time to market, it does not integrate other controls.
Independence	1	The control is performed by the people responsible for each of the two functions who are in a condition to independently manage all necessary resources.
Segregation	2	The head of the production department is not responsible for the determination of the market requisites, and the head of the quality department is not responsible for production cost containment. Both share the responsibility of compliance to norms and regulations.
Automation	4	Only the gathering of input data is supported by information systems.
Adaptability	1	The activity does not present variability in transaction volume to be managed. The control is thus capable of covering maximum volumes consistently.
Traceability	5	Only the input and output, if applicable, are recorded through information systems and thus traceable.
Overall strength of control	2.6	<i>The overall evaluation of strength of the control is based, in this case, on the simple average of the individual criteria.</i>
Relevance	2	While the correction of errors is specific to the control objective, the standards and the identification of errors is limited to production times and do not address storage or shipping aspects, which certainly impact the overall time-to-market objective.
Timeliness	5	The standard set for the control is reviewed only annually on the basis of specific needs or historical information.
Overall design of control	3.2	<i>The overall evaluation of strength of the control is based, in this case, on the simple average of the individual criteria.</i>

The overall evaluation of the internal control system design is adequate (rated at *three*) based on the evaluation of the two controls identified. This evaluation is strictly in relation to the control objective of ensuring compliance with time-to-market requirements.

However, it should be noted that the evaluation must be extended to the more general control objective—*ensuring product quality*. This control objective includes both guaranteeing achievement of time-to-market quality standards and conservation of the product at appropriate temperatures. In this (extreme) business case, no internal controls were identified in relation to the second control objective. This control objective is considered to be of equal risk and priority as the time-to-market

objective. Thus, in assessing the coverage criteria at process level, the evaluation would result in a rating of *four* because only one of the two control objectives is covered.

Such a situation would be unacceptable to an organization, which would expect full coverage of quality control objectives. Thus, the overall evaluation could result in a rating of *inadequate*. Exhibit 5.5 demonstrates the assessment of an inadequate control system.

Exhibit 5.5: Inadequate Control		
Control	Rules	Assessment rating (1 optimal - 5 negative)
1. Control of production time		2.3
2. Defining production time standards		3.2
Overall assessment of single controls	a	2.7
Overall assessment of coverage		4
Cost benefit factor		<i>not analyzed</i>
Overall assessment of internal control system of the process with regard to quality control	b	4

Assessment Rules:

- Average; no adjustment factors were applied.
- If coverage is rated worse than *two*, overall assessment cannot be better than *four*.

A rating of *four* is expressed as:

Inadequate internal control system, subject to significant improvements

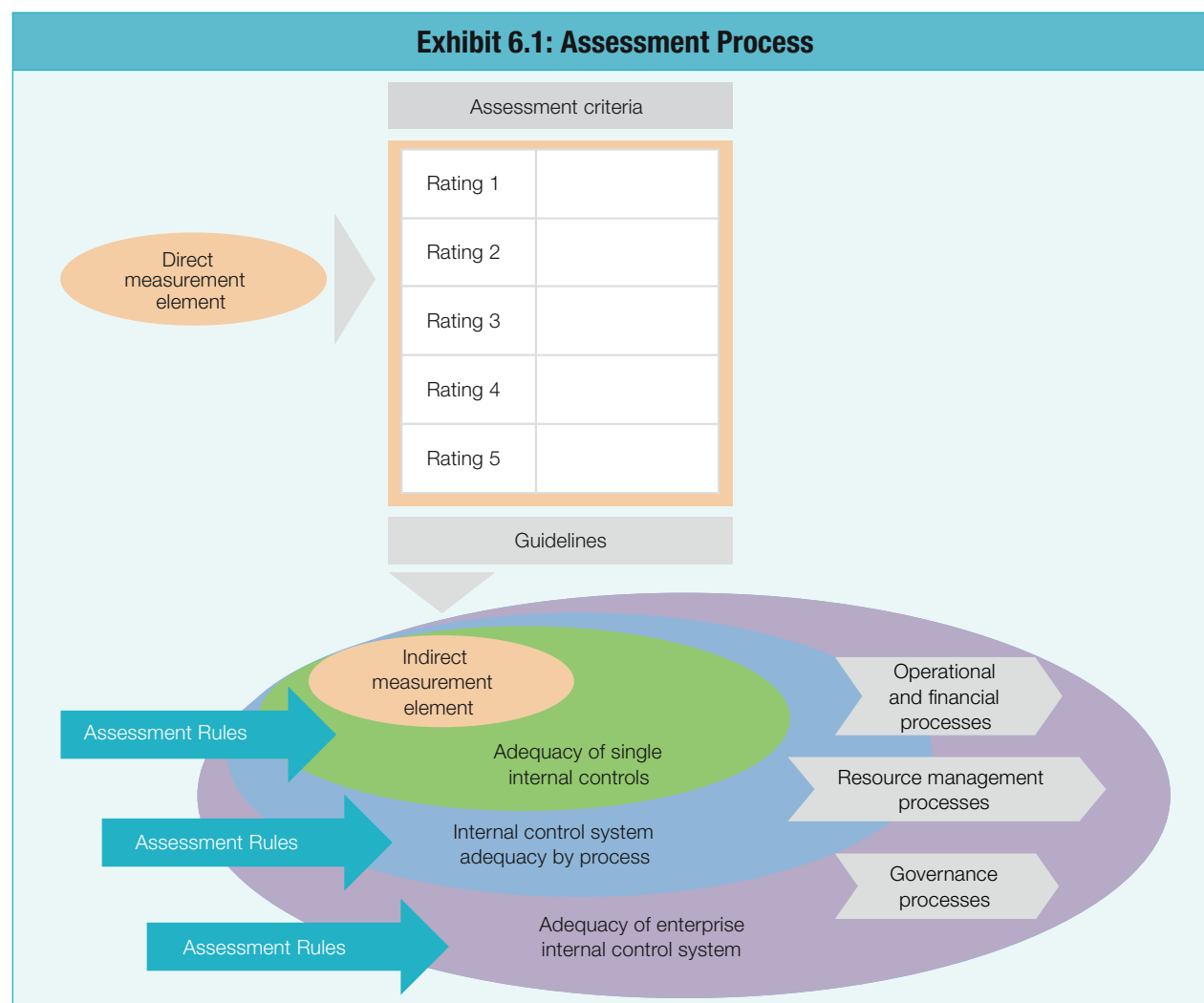
The controls only partially achieve the quality control objectives intended to mitigate the risks correlated to the business and governance objectives relevant to the production process based on risk management strategy.

ENTERPRISE-LEVEL ASSESSMENT

The evaluation of internal controls using the criteria and methodology provided by CAM should be applied consistently for each key process within the organization's business model. A full enterprise assessment is possible due to the aggregation and overall analysis of the internal control systems by key process.

The key to objectivity in the assessment process is using predefined criteria for establishing the ratings at various levels of complexity: control, process, entity. Exhibit 6.1 demonstrates the process flow

from direct measurement to rating assessment criteria through to the evaluation of adequacy and development of assessment rules.



The guidelines for enterprise-level ratings may introduce weighting factors or other rules according to experience or additional information.

Examples of weighting factors for each process to be considered include:

- Importance attributed to certain business or governance objectives associated to the process
- Presence of legislation or norms around certain control objectives
- Number and significance of risks associated with the process
- How recent the process assessment is
- Other nonrisk context variables

Once again, one of the greatest benefits of CAM is the objectivity and consistency of the criteria applied, as well as its applicability at any level of complexity. The approach is formalized and readily shared with interested parties. The complexity of the rules will develop based on accumulated experience and needs.

NOTES

1. For example, European Union directives give the audit committee responsibility for overseeing risk management, internal control, and internal audit. National Corporate Governance Codes issued by stock exchanges or regulatory authorities consistently request reporting on the adequacy of internal control and risk governance processes, and on corporate governance in general, under the principle of comply or explain.
2. See The IIA's Position Paper, *The Three Lines of Defense in Effective Risk Management and Control*, January 2013.
3. For example, the COSO framework on internal control provided by the Committee of Sponsoring Organizations of the Treadway Commission, Committee on Control Criteria (CoCo), etc.
4. Enterprise Risk Management (ERM) – Integrated Framework, Committee of Sponsoring Organizations of the Treadway Commission, September 2004.
5. For purposes of this paper, the terms *risk mitigation objective* and *control objective* are used synonymously. Internal controls are risk-based and designed to provide reasonable assurance regarding the achievement of objectives related to the business and governance objectives as defined by COSO.
6. This methodology is fully compliant with the requirements for a quality management system defined by the International Organization for Standardization (ISO). ISO 9001:2000 promoted the adoption of a process approach when developing, implementing, and improving the effectiveness of a quality management system to enhance customer satisfaction by meeting customer requirements.
7. This is a purely exemplary rating from *one* to *five* consolidating probability and impact factors. As noted, risk assessment techniques are not part of the scope of this document.
8. The control components consist of the identification of actual negative events or circumstances, its measurement, the comparison with the standard or desired outcome, and the correction process.
9. In the case of the internal auditor, this would, in principle, be in contrast with the auditor's right to full access of all records and information.
10. Discretion of control, segregation, independence, integration with other processes, automation, adaptability, and traceability.

THE IIA RESEARCH FOUNDATION SPONSOR RECOGNITION

The Mission of The IIA Research Foundation is to shape, advance, and expand knowledge of internal auditing by providing relevant research and educational products to the profession globally. As a separate, tax-exempt organization, The Foundation depends on contributions from IIA chapters/institutes, individuals, and organizations. Thank you to the following donors:

STRATEGIC PARTNER



PRINCIPAL PARTNERS



DIAMOND PARTNERS (US \$25,000+)



PLATINUM PARTNERS (US \$15,000–\$24,999)



GOLD PARTNERS (US \$5,000–\$14,999)



Stephen D. Goepfert, CIA, CRMA

SILVER PARTNERS (US \$1,000–\$4,999)

Anthony J. Ridley, CIA	IIA–San Antonio Chapter
Bonnie L. Ulmer	IIA–San Gabriel Chapter
Edward C. Pitts	IIA–San Jose Chapter
Hal A. Garyn, CIA, CRMA	IIA–Southern New England Chapter
IIA–Ak-Sar-Ben Chapter	IIA–St. Louis Chapter
IIA–Albany Chapter	IIA–Tidewater Chapter
IIA–Atlanta Chapter	IIA–Twin Cities Chapter
IIA–Baltimore Chapter	IIA–Vancouver Chapter
IIA–Birmingham Chapter	IIA–Western Carolinas Chapter
IIA–Calgary Chapter	IIA–Wichita Chapter
IIA–Central Illinois Chapter	Kevin M. Mayeux, CRMA
IIA–Indianapolis Chapter	Margaret P. Bastolla, CIA, CRMA
IIA–Lehigh Valley Chapter	Mark J. Pearson, CIA
IIA–Long Island Chapter	Michael J. Palmer, CIA
IIA–Miami Chapter	Paul J. Sobel, CIA, CRMA
IIA–Northern California East Bay Chapter	Richard F. Chambers, CIA, CCSA, CGAP, CRMA
IIA–Northwest Metro Chicago Chapter	Terri Freeman, CIA, CRMA
IIA–Ocean State Chapter	Urton L. Anderson, CIA, CCSA, CFSA, CGAP, CRMA
IIA–Pittsburgh Chapter	Wayne G. Moore, CIA
IIA–Sacramento Chapter	

THE IIA RESEARCH FOUNDATION BOARD OF TRUSTEES



PRESIDENT

Frank M. O'Brien, CIA, *Olin Corporation*

VICE PRESIDENT-STRATEGY

Michael F. Pryal, CIA, *Federal Signal Corporation*

VICE PRESIDENT-RESEARCH AND EDUCATION

Urton L. Anderson, PhD, CIA, CCSA, CFSA, CGAP,
University of Kentucky

VICE PRESIDENT-DEVELOPMENT

Betty L. McPhilimy, CIA, CRMA,
Northwestern University

TREASURER

Mark J. Pearson, CIA, *Boise, Inc.*

SECRETARY

Scott J. Feltner, CIA, *Kohler Company*

STAFF LIAISON

Margie P. Bastolla, CIA, CRMA,
The Institute of Internal Auditors Research Foundation

MEMBERS

Neil D. Aaron,
News Corporation

Fatimah Abu Bakar, CIA, CCSA, CRMA,
Columbus Advisory SDN BHD

Audley L. Bell, CIA,
World Vision International

Jean Coroller,
The French Institute of Directors

Edward M. Dudley, CIA, CRMA,
ABB North America

Philip E. Flora, CIA, CCSA,
FloBiz & Associates, LLC

Steven E. Jameson, CIA, CCSA, CFSA, CRMA,
Community Trust Bank

Jacques R. Lapointe, CIA, CGAP

James A. LaTorre,
PricewaterhouseCoopers LLP USA

Kasurthrie Justine Mazzocco,
IIA-South Africa

Guenther Meggeneder, CIA, CRMA,
ista International

Larry E. Rittenberg, PhD, CIA,
University of Wisconsin

Sakiko Sakai, CIA, CCSA, CFSA, CRMA,
Infinity Consulting

Mark L. Salamasick, CIA, CRMA,
University of Texas at Dallas

Jacqueline K. Wagner, CIA,
Ernst & Young LLP

William C. Watts, CIA, CRMA,
Crowe Horwath LLP



THE IIA RESEARCH FOUNDATION COMMITTEE OF RESEARCH AND EDUCATION ADVISORS



CHAIRMAN

Urton L. Anderson, PhD, CIA, CCSA, CFSA, CGAP, *University of Kentucky*

VICE-CHAIRMAN

Frank M. O'Brien, CIA, *Olin Corporation*

STAFF LIAISON

Lillian McAnally, *The Institute of Internal Auditors Research Foundation*

MEMBERS

Barry B. Ackers, CIA, *University of South Africa*
James A. Alexander, CIA, *Unitus Community Credit Union*
Sebastien Allaire, CIA, *Deloitte & Touche LLP (France)*
John Beeler, *SalesForce.com Inc.*
Karen Begelfer, CIA, CRMA, *Sprint Nextel Corporation*
Sharon Bell, CIA, *Wal-Mart Stores, Inc.*
Toby Bishop
Sezer Bozkus, CIA, CFSA, CRMA, *Grant Thornton Turkey*
John K. Brackett, CFSA, *McGladrey LLP*
Adil S. Buhariwalla, CIA, CRMA, *Emirates Airlines*
Richard R. Clune Jr., CIA, *Kennesaw State University*
Peter Funck, *Swedish Transport Administration*
Stephen G. Goodson, CIA, CCSA, CGAP, CRMA, *Texas Department of Public Safety*
Ulrich Hahn, PhD, CIA, CCSA, CGAP
Karin L. Hill, CIA, CGAP, CRMA, *Texas Department of Assistive and Rehabilitative Services*
Warren Kenneth Jenkins Jr., CIA, *Lowe's Companies, Inc.*
Jie Ju, *Nanjing Audit University*
Brian Daniel Lay, CRMA, *Ernst & Young LLP*
David J. MacCabe, CIA, CGAP, CRMA
Steve Mar, CFSA, *Nordstrom*
Jozua Francois Martins, CIA, CRMA, *Citizens Property Insurance Corporation*
John D. McLaughlin, *BDO*
Deborah L. Munoz, CIA, *CalPortland Cement Company*
Jason Philibert, CIA, CRMA, *TriNet*
Charles T. Saunders, PhD, CIA, CCSA, *Franklin University*
Rui Bezerra Silva, *Ventura Petroleo S.A.*
Tania Stegemann, CIA, CCSA, *Leighton Holdings Limited*
Warren W. Stippich Jr., CIA, CRMA, *Grant Thornton Chicago*
Deanna F. Sullivan, CIA, *SullivanSolutions*
Jason Thogmartin, *GE Capital Internal Audit*
Dawn M. Vogel, CIA, CRMA, *Great Lakes Higher Education Corporation*
Paul L. Walker, *St. John's University*
David Williams, *Dallas County Community College*
Valerie Wolbrueck, CIA, CRMA, *Lennox International, Inc.*
Douglas E. Ziegenfuss, PhD, CIA, CCSA, CRMA, *Old Dominion University*



