

Connect › Support › Advance

Whitepaper

Control Assessment: A Framework

JANUARY 2019

Control Assessment: A Framework

Contents

Background	2
- Purpose	2
- Background	2
Discussion	2
- Issue	2
- Adequate Control	3
- Reasonable Assurance	3
- Control Framework	3
- Assessment Model	4
- Documentation	4
Conclusion	4
- How to proceed	4
- Summary	5
- Conclusion	5
Bibliography	5
Acknowledgement	5
Purpose of White Papers	6
Author's Biography	6
About the Institute of Internal Auditors–Australia	6
Copyright	6
Disclaimer	6

Background

Purpose

Internal auditors are frequently called upon to assess whether a set of controls is 'adequate' to address risk. This is a process that requires considerable professional judgement, but there is little literature available to assist the internal auditor in making this assessment.

This judgement is an early, critical, decision point in the internal audit process. Getting the assessment wrong can lead to non-achievement of audit objectives and wasted resources.

This White Paper outlines a structured approach to analysis of individual controls against relevant risks, and points to a way that the auditor can make the necessary assessment.

The same process can be applied in assessing whether a proposed control will address an identified gap.

Background

A control is any action taken by management to enhance the likelihood that objectives will be achieved. A control is intended to manage risk. Controls can be classified in many ways. These classifications help us understand the nature and purpose of the control.

Controls may be:

- Preventive – to deter undesirable events from occurring.
- Detective/Corrective – to detect and correct undesirable events that have happened.
- Directive – to cause or encourage a desirable event to occur.

Controls may be 'hard controls' or 'soft controls':

- Hard controls are formal controls such as policies and procedures, reconciliations of accounting records, management sign-offs, a documented business plan, written code of conduct, separation of duties, and safety procedures.
- Soft controls are informal and include competency, knowledge and understanding of employees, ethical behaviour of management and staff, relationship building, and employee understanding of procedures.

Soft controls are more difficult to audit than hard controls because generally there are no clear and definitive methods of testing them.

Controls may be:

- Automated – technological controls that are designed to function in a specific way under predetermined conditions.
- Manual – controls that require the intervention of a person or group of people.

To manage risks, organisations apply both controls that typically fall into three layers:

- Systems and processes.
- Capability.
- Culture – leadership, behaviour, attitudes.

Discussion

In this context, a control system is 'adequate' if:

"... management has planned and organized (designed) in a manner that provides reasonable assurance that the organization's risks have been managed effectively and that the organization's goals and objectives will be achieved efficiently and economically".

Source: Glossary to the 'International Professional Practices Framework', IIA–Global.

Control Assessment: A Framework

Internal auditors are obliged by Standard 2320 (Analysis and Evaluation) to “base conclusions and engagement results on appropriate analyses and evaluations”.

This approach provides the internal auditor with a framework for making the necessary analyses and evaluations.

Adequate Control

Looking closer at the definition of adequate, we note a number of phrases:

- ‘Control system’ – The definition applies to groups of controls: not to individual controls. While it is possible that a single control may form an adequate control system, it is highly unlikely.
- ‘Planned and organised’ – The statement is about the design of the control system: not about its operation. A control does not necessarily have the intended effect and any effect must be verified by testing.
- ‘Reasonable assurance’ – Controls are designed to reduce uncertainty (variation) in performance but they cannot eliminate it.
- ‘Efficiently and economically’ – This implies that inefficient control – even if effective – is not adequate.

Recognising that risk is only an expression of the uncertainty organisations face in achieving objectives, control systems, too, are focused on objectives. An adequate control system promotes the achievement of objectives by managing specific risks.

Reasonable Assurance

According to Committee of Sponsoring Organizations (COSO):

“The term ‘reasonable assurance’ rather than ‘absolute assurance’ acknowledges that limitations exist in all systems of internal control, and that uncertainties and risks may exist, which no one can confidently predict with precision. Absolute assurance is not possible. Reasonable assurance does not imply that an organisation will always achieve its objectives”.

Source: Committee of Sponsoring Organizations, 2013.

The question that is not addressed is: what does ‘reasonable’ mean? Dictionary meanings include: ‘fair and sensible’ or ‘as much as is appropriate’. These definitions do not help much, because they rely on the meaning of ‘appropriate’: suitable or proper in the circumstances.

In other words, what is reasonable is a matter of judgment. To make the judgement, one must ask: how much does the objective matter? Controls that affect life or safety must be

stronger than controls that manage a small inventory. One interpretation of ‘reasonable assurance’ in relation to a financial statement figure is that the probability of a material error not being detected by the controls is no more than 5-10% (Marks & et al, 2008, p 57).

The auditor must decide for themselves how much control provides reasonable assurance. This is a decision that requires conscious thought.

Control Framework

COSO (Committee of Sponsoring Organizations, 2013) has provided a useful control framework that teaches us controls are always in relation to a risk, and that risk is always in relation to objectives in the context of the organisation. Controls exist in a framework that has five components:

1. Control Environment – the set of standards, processes, and structures that provide the basis for carrying out internal control across the organisation.
2. Risk Assessment – a dynamic and iterative process for identifying and analysing risks associated with the organisation’s objectives.
3. Control Activities – actions established by policies and procedures to help ensure that risks to the achievement of objectives are managed.
4. Information and Communication – information is necessary for the organisation to carry out internal control responsibilities in support of its objectives. Communication provides the organisation with the information needed to carry out day-to-day controls; it enables personnel to understand internal control responsibilities and their importance.
5. Monitoring Activities – monitoring activities ascertain whether each of the five components of internal control is present and functioning.

This model makes it clear that control design is not only about so-called hard controls – processes and procedures – but also encompasses soft controls such as competency, ethics, and internal discipline and culture. It is also clear that procedures to monitor the performance of controls are a necessary part of the control design.

Control Assessment: A Framework

Assessment Model

In the assessment model, control design is assessed against six independent characteristics, and in relation to specific objectives and their associated risks.

No.	Factor	Description
1	Relevance	<p>Does the proposed control address a risk that matters? Does the listed control actually address the risk that it is listed against?</p> <p>The control may be valuable for other reasons, but it is not contributing to the control of the specified risk(s). It does not therefore contribute to the adequacy of the control system in the process under consideration.</p>
2	Coverage	<p>Does the proposed control address part of a risk, all of a risk, or a number of risks?</p> <p>Where a control is addressing only part of a risk, it may be best to restructure the risk so that the part where the control is function is separate from the rest. It is quite common for a particular control to address more than one risk and this, when possible, can have cost advantages.</p>
3	Strength/Reliability	<p>Will the control work every time – is it independent of the process, is it automated, does it prevent an issue, correct an issue or just identify an issue?</p> <p>A preventive control is clearly preferable, but is not always possible. A detective control always requires some response mechanism. Automated controls always perform as constructed – this may be desirable if the construction is sound, but some circumstances may require human judgement and this aspect should not be ignored.</p>
4	Reactivity	<p>Does the control operate quickly enough to minimise adverse consequences?</p> <p>A control intended to limit the effects of, or take advantage of, an event, must operate at an appropriate speed. If the action is too late, it is ineffective.</p>
5	Resource availability	<p>Does the organisation have the competence or resources to operate the control?</p> <p>Is it an additional piece of work for an already busy person?</p> <p>These are design questions with a direct performance implication. Some controls are intrinsically complex and require expertise to perform correctly. Giving the responsibility to a person without that expertise reduces or eliminates the value of the control. Similarly, if an individual, or group of individuals, is given too much to do, they will set priorities that may eliminate or reduce the control's operation.</p>
6	Exception analysis	<p>Is the operation of the control monitored and analysed?</p> <p>What happens to rejected items?</p> <p>Is there a mechanism in place to manage unusual circumstances? Are there performance reports that might help the organisation detect changes in risk?</p>

It is unlikely a single control will meet all the characteristics when considered in relation to a particular risk. Consequently, it is usual to use a combination of controls. For example, reconciliations are put in place to detect when other accounting controls, that depend on the activities of individuals, have not operated correctly. Similarly, audible alarms are used to alert people should a security door be left open.

This assessment framework still relies on the judgement of the auditor. It provides the auditor with a mechanism to formally consider each aspect of control design, and provides a basis for making the assessment of whether a control system is adequate.

Documentation

You may consider documenting your assessment of controls in the following manner:

Risk	Control	Control Analysis						Test Control?
		Relevance	Coverage	Strength	Reactivity	Resource	Exception	
xxx	xxx	Yes	Full	Strong	Sufficient	No	Yes	Yes
	xxx	Yes	Full	Weak	Fast	Yes	Yes	Yes

Clearly, there is only limited value in testing controls that do not contribute to an adequate control set. Nevertheless, there is sometimes value in this activity when assessing how much additional control is needed.

Conclusion

How to proceed

This technique can be integrated with your existing service offerings.

- In reviews of existing systems or processes, the technique may be used to consider the control design before testing is undertaken. Testing can be focused on those controls that are most important in the context of the review.
- Similarly, in the review of proposed systems, the control design may be formally assessed against the system risks. The decision about adequacy can be based on structured analysis.
- It may be used in the development of new controls – when developing recommendations or when advising on new activities – by choosing controls with appropriate characteristics.

Control Assessment: A Framework

Summary

This White Paper outlines a structured approach to analysis of individual controls against relevant risks, and points to a way that the auditor can make the necessary assessment.

The same process can be applied in assessing whether a proposed control will address an identified gap.

Conclusion

By assessing internal controls, whether in place or proposed, against the six characteristics in this framework, the internal auditor is taking a structured approach to analysis and evaluation of the controls.

This will facilitate collection of necessary evidence, and assist in answering the question of whether controls are, or can be made, 'adequate'.

Bibliography and References

Acknowledgement

This approach is based upon a framework developed by Poste Italiane, and presented to the IIA International Conference in Kuala Lumpur in 2011. The Poste Italiane framework has been more fully developed in an IIA Research Foundation publication (Dittmeier & Casati, 2014).

References

Committee of Sponsoring Organizations. (2013, May). Internal Control - Integrated Framework. COSO. Retrieved from http://www.coso.org/documents/990025P_Executive_Summary_final_may20_e.pdf

Dittmeier, C., & Casati, P. (2014). Evaluating Internal Control Systems: A Comprehensive Assessment Model for Enterprise Risk Management. Altamonte Springs FL, United States of America: The Institute of Internal Auditors Research Foundation.

Institute of Internal Auditors. (2016, October). International Standards for the Professional Practice of Internal Auditing. (IIASB, Ed.) Retrieved from The Institute of Internal Auditors - Global: <https://global.theiia.org/standards-guidance/Public%20Documents/IPPF-Standards-2017.pdf>

Marks, N., & et al. (2008). SARBANES-OXLEY SECTION 404: A Guide for Management by Internal Controls Practitioners (2nd ed.). Institute of Internal Auditors, Inc. Retrieved from https://na.theiia.org/standards-guidance/Public%20Documents/Sarbanes-Oxley_Section_404_--_A_Guide_for_Management_2nd_edition_1_08.pdf

Control Assessment: A Framework

Purpose of White Papers

A White Paper is an authoritative report or guide that informs readers concisely about a complex issue and presents the issuing body's philosophy on the matter. It is meant to help readers understand an issue, solve a problem, or make a decision.

Author's Biography

Written by: Michael Parkinson
BSc (Hons), GradDipComputing, CIA, CISA, CRMA, CRISC

Michael is an internal auditor and risk management consultant in private practice. He has more than 30 years of experience in a range of government and non-government environments. He has been active in the development of risk management and internal auditing standards and guidance for more than 10 years. Michael has practiced in Australia and South-East Asia, and currently serves on a number of Audit and Risk Management Committees.

Michael has been the recipient of the IIA–Australia Bob McDonald Award and the IIA–Global Victor Z Brink Award for services to the profession of internal auditing.

Edited by: Andrew Cox
MBA, MEC, GradDipSc, GradCertPA, DipBusAdmin,
DipPubAdmin, AssDipAcctg, CertSQM, PFIIA, CIA, CISA, CFE,
CGAP, CSQA, MACS Snr, MRMIA

About the Institute of Internal Auditors–Australia

The Institute of Internal Auditors (IIA) is the global professional association for Internal Auditors, with global headquarters in the USA and affiliated Institutes and Chapters throughout the world including Australia.

As the chief advocate of the Internal Audit profession, the IIA serves as the profession's international standard-setter, sole provider of globally accepted internal auditing certifications, and principal researcher and educator.

The IIA sets the bar for Internal Audit integrity and professionalism around the world with its 'International Professional Practices Framework' (IPPF), a collection of guidance that includes the 'International Standards for the Professional Practice of Internal Auditing' and the 'Code of Ethics'.

The IPPF provides a globally accepted rigorous basis for the operation of an Internal Audit function. Procedures for the mandatory provisions require public exposure and formal consideration of comments received from IIA members and non-members alike. The standards development process is supervised by an independent body, the IPPF Oversight

Council of the IIA, which is appointed by the IIA–Global Board of Directors and comprises persons representing stakeholders such as boards, management, public and private sector auditors, regulators and government authorities, investors, international entities, and members specifically selected by the IIA–Global Board of Directors.

IIA–Australia ensures its members and the profession as a whole are well-represented with decision-makers and influencers, and is extensively represented on a number of global committees and prominent working groups in Australia and internationally.

The IIA was established in 1941 and now has more than 180,000 members from 190 countries with hundreds of local area Chapters. Generally, members work in internal auditing, risk management, governance, internal control, information technology audit, education, and security.

Copyright

This White Paper contains a variety of copyright material. Some of this is the intellectual property of the author, some is owned by the Institute of Internal Auditors–Global or the Institute of Internal Auditors–Australia. Some material is owned by others which is shown through attribution and referencing. Some material is in the public domain. Except for material which is unambiguously and unarguably in the public domain, only material owned by the Institute of Internal Auditors–Global and the Institute of Internal Auditors–Australia, and so indicated, may be copied, provided that textual and graphical content are not altered and the source is acknowledged. The Institute of Internal Auditors–Australia reserves the right to revoke that permission at any time. Permission is not given for any commercial use or sale of the material.

Disclaimer

Whilst the Institute of Internal Auditors–Australia has attempted to ensure the information in this White Paper is as accurate as possible, the information is for personal and educational use only, and is provided in good faith without any express or implied warranty. There is no guarantee given to the accuracy or currency of information contained in this White Paper. The Institute of Internal Auditors–Australia does not accept responsibility for any loss or damage occasioned by use of the information contained in this White Paper.