Risk-based internal auditing – is your organisation ready?

According to the results of external quality assessments by the Chartered IIA, some audit leaders do not position the work of internal audit within the context of an organisation's risk framework. There may be good reason for this, but it can also be due to lack of awareness.

The phrase 'risk based internal auditing' (RBIA) has become commonplace since its introduction in 2005 and applies to all sectors. It is one of those taken for granted assumptions that everyone understands what it is.

In this article, we explore the question so you can answer it for yourself. We will get back to basics taking a look at what it really means, when to use it and what to do if your organisation is not quite ready for it.

Short for time? Skip ahead to ten reasons to embrace RBIA.

RBIA defined

The Institute defines RBIA as a methodology that links internal auditing to an organisation's overall risk management framework.

It is not as simple as auditing the top risks on the organisations risk register!

RBIA provides assurance that risks are being managed within a defined risk appetite.

Using this approach, internal audit can report on the effectiveness and efficiency of the processes, polices

and governance in place to manage risks to the level considered acceptable by the board.

The key to RBIA is risk management: specifically the maturity of the organisation's approach to it.

RBIA goes beyond the traditional approach of auditing objectives, processes, controls; it audits risk. By establishing the risks to achieving objectives it enables internal audit to align directly with the purpose of the organisation.

A RBIA methodology has three important stages. Firstly, in assessing the organisations risk maturity and the reliability of risk information produced by management. Secondly, at a strategic level it determines the 'annual' audit plan and then thirdly at an operational level it guides the individual audit engagements.

- Do you think about RBIA in this way?
- Have you considered doing RBIA?
- Do you do this already?

Assessing risk maturity

An organisation's risk framework should be formal regardless of whether or not it adopts a standard such as ISO31000. Every organisation is unique in terms of its risks and often its approach to risk management. Maturity is the term used for how well the concept has been adopted, evidenced through the framework.

The Institute defines five levels of risk maturity.

Audit leaders should assess their organisation's risk maturity.

Two aspects of the risk framework are of paramount importance in relation to RBIA: risk appetite and risk assessment.

Risk Appetite

The board decide how much risk the organisation can take in pursuit of its strategy. This, in turn, sets the parameters for management decision-making in the day to day running of the organisation; the opportunities to be taken and threats to be minimised.

RBIA uses risk appetite as a stake in the ground - the fulcrum of decision-making. Without a defined risk appetite, providing assurance on the effective management of risk can be very subjective – a battle of opinion between internal audit and the business, including second line functions such as risk.

Risk Assessment

As with any methodology, audit leaders need to be able to prioritise their resources. For RBIA, that requires the assessment of risks at both the inherent and residual level – something that not all organisations are willing or skilled enough to engage with. Whilst it is the ideal, audit leaders should not be put off in its absence; internal audit may find it useful to work with second line functions to educate and promote the concept. Risk severity on its own only tells part of the story.

Providing assurance that risks are effectively and efficiently managed from their inherent level to within an acceptable risk appetite is the premise of RBIA. Internal audit effort focuses on risk treatments being proportionate and also calling out those that risks that remain in excess of risk appetite.

- Has your organisation's risk maturity been assessed?
- Does your audit strategy match the maturity?
- Do you formally assess against risk appetite?

Maturity and audit strategy

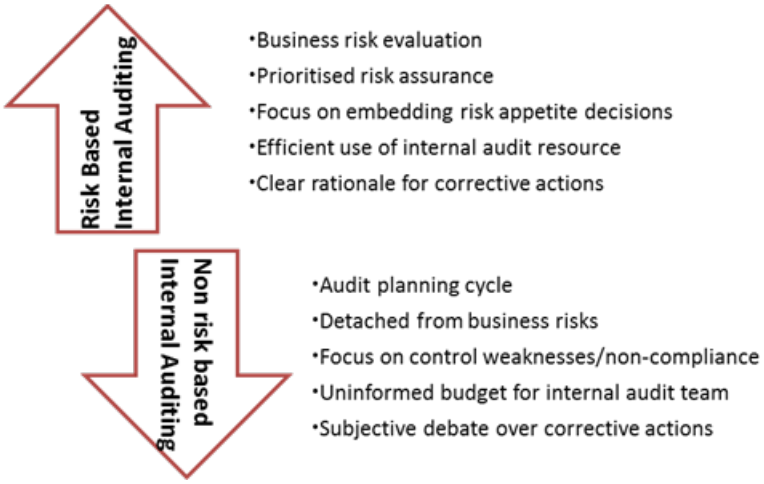
In the absence of a suitable risk management framework, internal audit can only provide control-based assurance. It is not possible to provide risk-based assurance when the organisation has not appropriately identified or assessed its own risks. This does not preclude relating audit findings to risks, recognising that these will have been identified by internal audit or through ad hoc management processes.

The following table outlines key elements of the audit strategy in relation to an organisation's level of risk maturity.

Maturity	Key Characteristics	Internal Audit Approach
Naïve	No formal approach developed for risk management	-Report no formal risk management -Consulting to champion risk management -Audit plan driven by alternate framework (IA informed) -Assurance on control processes
Aware	Scattered silo based approach to risk management	-Report poor risk management - Consulting to champion risk management -Audit plan driven by alternate framework (IA informed) -Assurance on control processes
Defined	Strategy and policies in place and communicated. Risk appetite defined	-Report risk management deficiencies -Audit plan starts with managements view of risk then supplement -Assurance control processes and on risk management policies -Consulting to embed risk management
Managed	Enterprise wide approach to risk management developed and communicated	-Managements view of risk drives audit plan -Assurance on risk management processes and mitigation -Consulting to improve risk management
Enabled	Risk management and internal control fully embedded into the operations	-Managements view of risk drives audit plan -Assurance on risk management processes and mitigation -Consulting as requested

RBIA assurance

Audit leaders should discuss the transition to RBIA with their audit committee as the methodology influences internal audit activities at both a strategic and operational level.



Strategic – audit plan

The Institute provides detailed guidance on producing an audit plan for audit leaders wanting to adopt RBIA.

Annual plans are often rolling or regularly updated due to the volatility of risks. Auditors must also be able to react quickly to the emerging assurance needs of their organisation; having the skills to use an agile methodology may be of value.

It could be useful to describe the audit plan in relation to the three lines of defence model: linking independent assurance to where the risks are being managed in the first and second lines. Positioning assurance and consultancy activity in the third line for topics such as reputation and culture clearly demonstrates the unique role of internal audit in providing independent support to the board on strategic matters.

The organisation's risk appetite is key to RBIA and whilst it is not internal audit's role to question the appetite itself, audit leaders must regularly assure themselves that the process to determine it is effective. Risk appetite is fluid and should be adjusted when material factors change such as financial performance issues, Brexit, new board members and stakeholder expectations.

It is important to remember that risk is also about opportunity and how it is effectively managed as much as it is about threats to be mitigated. Audit leaders should ensure their team are skilled in risk management in addition to the traditional audit skills.

Operational – audit engagement

The Institute provides detailed guidance on carrying out a RBIA audit engagement.

With RBIA, the focus of assurance is on how risks are managed, specifically that they are managed to within the risk appetite of the board. Not best practice or the opinion of the auditor.

Auditors shift their emphasis away from checking operational controls and their effectiveness (such as authorisation of invoices) to checking that management controls which detect and action failures, the key operating controls, are effective. RBIA is a constant reminder of where risk is owned and managed.

- What does your audit committee think about RBIA?
- Would your executive team welcome this approach?
- Is your audit team sufficiently skilled to do this?

Aspiring to RBIA

Audit leaders in organisations with risk maturity at the naïve or aware levels should work closely with the audit committee to ensure that their expectations are realistic and their aspirations are as high as those of internal audit.

Assurance limitations

Without RBIA, internal audit is limited to providing control assurance.

The absence of risk information from the organisation requires internal audit to produce its own framework for determining an appropriate audit plan; perhaps a simple list of auditable areas or a robust audit universe.

Auditors must take care in the language and presentation of such information that this is not seen as a substitute for the organisation developing and embedding risk management processes.

Consultancy activity

Audit leaders should use their internal audit charter to set clear boundaries of accountability regarding risk management. There are many roles internal audit can legitimately undertake in supporting the organisation to raise its risk maturity.

Consultancy activity related to improving risk management should be regarded as an appropriate use of internal audit resource; audit committees should not be accepting risk maturity levels below 'defined'.

Audit leaders may wish to read a position paper that deals with internal audit also performing the function of risk management. It will help to protect the integrity of internal audit during the transition to maturity. This is not an uncommon scenario outside of financial services.

Promoting the benefits of RBIA to the audit committee will be helpful in creating positive expectations for the value internal audit can add to the organisation once the organisation adopts risk management.

Ten reasons to embrace RBIA

1. It is about auditing the management of risks not the risks themselves.
2. It ensures that internal audit resources are directed towards the most significant risks.
3. It prioritises the audit committee's assurance requirements.
4. It links internal audit assurance to the achievement of the organisation's objectives.
5. It justifies the number of internal auditors required.
6. It requires auditors with interviewing, influencing, facilitating and problem-solving skills.
7. It is an inclusive approach, partnering internal audit with the board.
8. It identifies residual risks that are not in line with risk appetite.
9. It facilitates the continuous improvement of risk mitigation strategies.
10. It prioritises corrective actions in line with the importance of risks.

Here are some additional questions for consideration:

- Are you striving to improve your organisation's risk maturity?
- Who are the champions on your executive team?
- Have you set a target to transition to RBIA?

Closing thoughts

Having looked at the building blocks for risk based internal auditing, it is clear that it cannot happen in isolation from the organisation, no matter how much the audit team may be ready to do it. In the quest for providing assurance that gets to the very heart of what matters the most, internal audit must partner with the audit committee to create an environment in which RBIA can be delivered and received.

"Without continuous effort there cannot be continuous achievement"

Dr Orison Swett Marden, philosopher and author

Further reading

Risk based internal audit planning in Financial Services

Risk maturity assessment

Implementing risk based internal auditing

RBIA production of the audit plan

What an effective risk based internal audit looks like

Doing a risk-based audit