Chartered Institute of
Internal Auditors

08 October 2014

Risk based internal auditing

Chartered Institute of Internal Auditors

Background

Over the last few years, the need to manage risks has become recognised as an essential part of good corporate governance practice. This has put organisations under increasing pressure to identify all the business risks they face and to explain how they manage them.

In fact, the activities involved in managing risks have been recognised as playing a central and essential role in maintaining a sound system of internal control.

While the responsibility for identifying and managing risks belongs to management, one of the key roles of internal audit is to provide assurance that those risks have been properly managed.

We believe that a professional internal audit activity can best achieve its mission as a cornerstone of governance by positioning its work in the context of the organisation's own risk management framework.

What is risk based auditing?

Our definition

IIA defines risk based internal auditing (RBIA) as a methodology that links internal auditing to an organisation's overall risk management framework. RBIA allows internal audit to provide assurance to the board that risk management processes are managing risks effectively, in relation to the risk appetite.

Is the organisation ready?

Every organisation is different, with a different attitude to risk, different structure, different processes and different language. Experienced internal auditors need to adapt these ideas to the structures, processes and language of their organisation in order to implement RBIA.

RBIA seeks at every stage to reinforce the responsibilities of management and the board for managing risk.

If the risk management framework is not very strong or does not exist, the organisation is not ready for RBIA. More importantly, it means that the organisation's system of internal control is poor. Internal auditors in such an organisation should promote good risk management practice to improve the system of internal control.

Where RBIA is new to an organisation, the head of internal audit will need to market the concept to management and win their support, particularly since it may mean a change for them in the way that they think about risk.

A dynamic process

RBIA is at the cutting edge of internal audit practice. As a result, it is an area that is evolving rapidly and where there is still little consensus about the best way to implement it.

It is more difficult to manage than traditional methodologies. Monitoring progress against an annual plan that is constantly changing is a challenge. Setting targets and appraising staff may become more complex.

But the advantages of RBIA are much greater.

Advantages

By following RBIA internal audit should be able to conclude that:

1. Management has identified, assessed and responded to risks above and below the risk appetite
2. The responses to risks are effective but not excessive in managing inherent risks within the risk appetite
3. Where residual risks are not in line with the risk appetite, action is being taken to remedy that
4. Risk management processes, including the effectiveness of responses and the completion of actions, are being monitored by management to ensure they continue to operate effectively
5. Risks, responses and actions are being properly classified and reported.

This enables internal audit to provide the board with assurance that it needs on three areas:

1. Risk management processes, both their design and how well they are working
2. Management of those risks classified as 'key', including the effectiveness of the controls and other responses to them
3. Complete, accurate and appropriate reporting and classification of risks

Read more about the benefits and drawbacks of RBIA

Implementation of RBIA

The implementation and ongoing operation of RBIA has three stages and we have produced detailed guidance on each of them:

Stage 1: Assessing risk maturity

Obtaining an overview of the extent to which the board and management determine, assess, manage and monitor risks. This provides an indication of the reliability of the risk register for audit planning purposes.

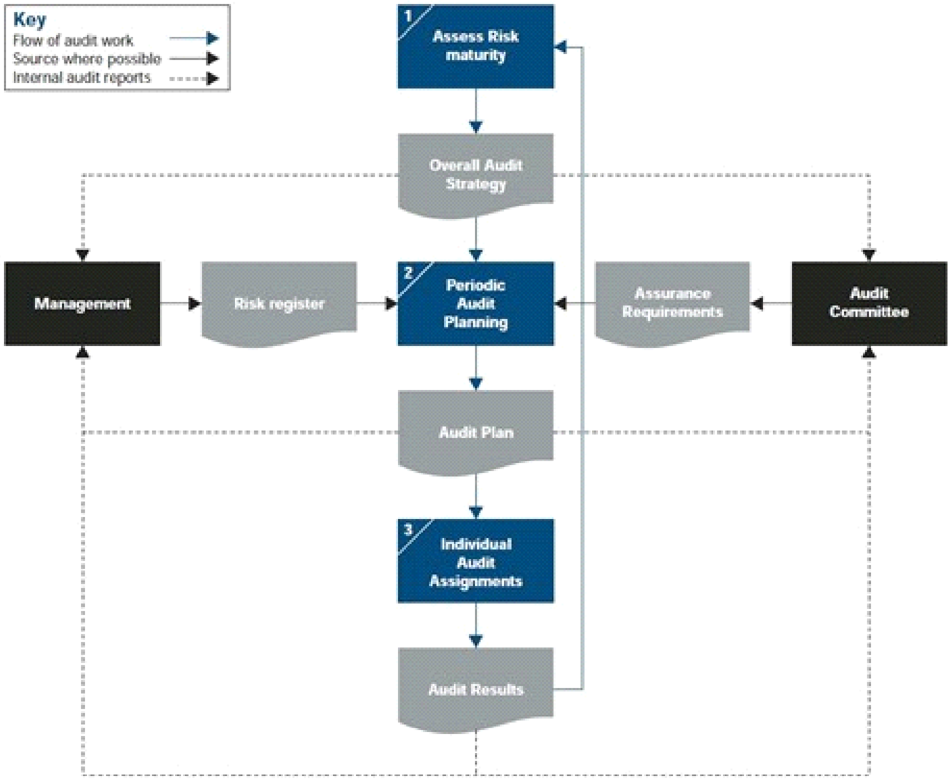
Stage 2: Periodic audit planning

Identifying the assurance and consulting assignments for a specific period, usually annual, by identifying and prioritising all those areas on which the board requires objective assurance, including the risk management processes, the management of key risks, and the recording and reporting of risks.

Stage 3: Individual audit assignments

Carrying out individual risk based assignments to provide assurance on part of the risk management framework, including on the mitigation of individual or groups of risks.

Overview of the stages



Expand this diagram

Next: Risk maturity assessment

Chartered Institute of
Internal Auditors

29 May 2014

Risk maturity assessment

Chartered Institute of Internal Auditors

The first stage of RBIA is to review the level of risk maturity. There are three objectives to this stage, which are to:

1. Assess the risk maturity of the organisation
2. Report to management and to the audit committee on that assessment
3. Agree an audit strategy

Actions to achieve the objectives

1. Discuss the understanding of risk maturity with the board and senior managers.

Determine what has already been done to improve the risk maturity of the organisation such as training, risk workshops, questionnaires about risks and interviews with risk managers.

Determine whether managers feel that the risk register is comprehensive. Discuss whether an understanding of risk management is embedded so that managers feel responsible not only for identifying, assessing and mitigating risks but also for monitoring the framework and the responses to risks.

2. Obtain documents, where they are available, which detail:

- The objectives of the organisation.
- How risks are analysed, for example by scoring their impact and likelihood.
- A definition, approved by the board, which defines its risk appetite in terms of the scoring system used for inherent and residual risks.
- The processes followed to identify risks which threaten the organisation's objectives.
- How management considers risks as part of their decision making. For example, including risks and the response to them, in project approval documents.
- The processes followed to report risks at different levels of management.
- The sources of information used by management and the board to assure themselves that the framework is working effectively to manage risks within the risk appetite.
- The risk register of the organisation, including the types of information described in the previous section.
- Any existing assessment by management or the board of the risk maturity of the organisation.
- Any other documents which indicate the commitment to risk management.

3. Conclude on the risk maturity.

Using the documents and information gathered, assess the organisation's risk maturity using these stages: risk enabled, risk managed, risk defined, risk aware and risk naïve.

Appendix A: Assessing the organisation's risk maturity provides these definitions and suggests the factors you can take into account to do this assessment. It also suggests audit tests that you can undertake to provide evidence to support your assessment.

4. Report your conclusion on risk maturity to management and to the audit committee.

This stage will provide a first, high level, assurance on the risk management processes, the management of key risks and on the recording and reporting of risks.

In reporting your conclusions and their implications, you should note that a risk maturity of risk naïve or risk aware implies that the organisation's system of internal control and the board's ability to assess it may be ineffective. The IIA believes that risk naïve and risk aware organisations are not complying with either the Turnbull Guidance or the Code of Corporate Governance.

5. Work with management to identify any actions they propose to take as a result of this assessment.

Management may suggest consulting assignments for internal audit such as, for example, facilitating management's efforts to improve their risk management processes.

6. Decide on the audit strategy

This will follow from your assessment and obtaining approval from management and audit committee.

Range of audit strategies

The audit strategy selected depends upon the organisation's risk maturity. Risk naïve or risk aware organisations will be unable to implement RBIA straight away. However, such organisations can benefit from some aspects of the audit strategies described below.

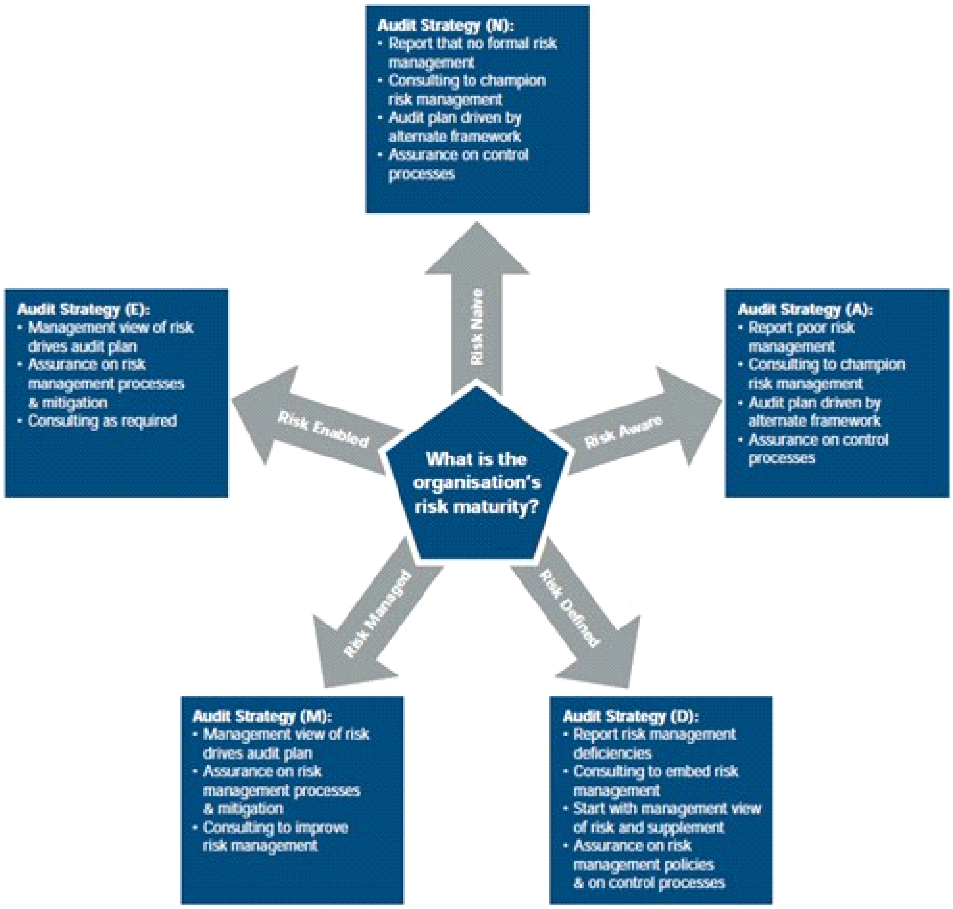
For example, internal audit can help improve risk management and governance processes by reporting its assessment of the risk maturity of the organisation to management and to the audit committee, and by championing risk management throughout the internal audit activity's work.

It may also conduct consulting assignments supporting management in improving the organisation's risk maturity.

There are three potential elements to an RBIA audit strategy:

1. the type of assurances that you expect to be able to give
2. the framework that will be used for your audit planning
3. the type of consulting services that you expect to provide.

RBIA Stage 1 - Range of audit strategies:


Audit Strategy (N):
• Report that no formal risk management
• Consulting to champion risk management
• Audit plan driven by alternate framework
• Assurance on control processes
Audit Strategy (E):
• Management view of risk drives audit plan
• Assurance on risk management processes & mitigation
• Consulting as required
Audit Strategy (A):
• Report poor risk management
• Consulting to champion risk management
• Audit plan driven by alternate framework
• Assurance on control processes
Risk Naive
Risk Enabled
Risk Aware
What is the organisation's risk maturity?
Risk Managed
Risk Defined
Audit Strategy (M):
• Management view of risk drives audit plan
• Assurance on risk management processes & mitigation
• Consulting to improve risk management
Audit Strategy (D):
• Report risk management deficiencies
• Consulting to embed risk management
• Start with management view of risk and supplement
• Assurance on risk management policies & on control processes

Expand this diagram

Assurance strategies

For risk enabled and risk managed organisations, the conclusion on risk maturity is the first step in being able to provide assurance on risk management processes, management of key risks and reporting of risks. The internal audit activity's assurance strategy is therefore to provide assurance on these areas.

For other organisations, the conclusion on risk maturity means that such assurances are not available.

Those in risk defined organisations may be able to identify risk management policies or pockets of risk management excellence and be able to plan to provide assurance on these elements.

Otherwise, internal audit should plan to provide assurance that control processes are working according to the objectives or standards that have previously been set.

Framework for audit planning

In risk enabled and risk managed organisations, RBIA means that audit planning is driven from the organisation's risk register and its need for objective assurance. This is described in greater detail in production of the audit plan.

For other organisations, there is no reliable risk register. Therefore, in these organisations, the internal audit activity will need to plan its audit work using an alternative framework, for example, key systems or business units.

In the past, internal auditors have performed their own assessments of the risks facing their organisations. It is tempting to take these assessments and start considering them the organisation's risk register.

However, this may be detrimental to the ultimate goal of improving the organisation's risk maturity since it is likely to reinforce the misconception that internal audit are responsible for risk management.

The RBIA methodology drives internal auditors to facilitate the improvement of the risk management framework.

Therefore, the use of misleading names, such as audit needs or risk assessments or analyses, should be discontinued in favour of the generic term 'audit planning framework'.

Consulting strategies

In less risk mature organisations, internal audit may wish to set aside time to champion the introduction and improvement of risk management processes. The aim of this type of consulting activity is to improve the risk maturity of the organisation.

Internal audit should approach the work in such a way that management retains a sense of ownership of the processes that are being developed.

The IIA's International Standards 4 define consulting activities as advisory services, the nature and scope of which are agreed with the client and which do not involve the internal auditor assuming any management responsibility. Our position statement on The Role of Internal Audit in Enterprise-wide Risk Management provides further guidance on the roles that you may undertake and those that you may not.

In risk enabled and risk managed organisations, the need to improve risk management processes is less pressing than in less risk mature organisations and may be part of the framework itself. As a result, less resource may be needed for consulting work.

Mixed risk maturities

It is possible that one part of an organisation may be risk managed and another risk aware. Alternatively, an organisation may be risk managed when it comes to one type of risk, for example, market risk in a bank, but risk aware for another type of risk.

In this case, internal audit should not conclude that the whole organisation is risk managed. It should report the dangers of having a patchwork of risk maturities and devise audit strategies separately for the different parts of the organisation.

Next: Production of the audit plan

Appendices

Guidance on implementing key aspects of RBIA methodology:

A: Assessing the organisation's risk maturity
B: Guidance on assigning audit conclusions

Illustrations of how you might document parts of the risk management framework and RBIA:

C: Risk register (part)
D: Audit universe (part)
E: Risk and audit universe (part)
F: Audit plan (April 2005 - March 2006)
G: Individual audit database for expense purchasing (part)

13 October 2014

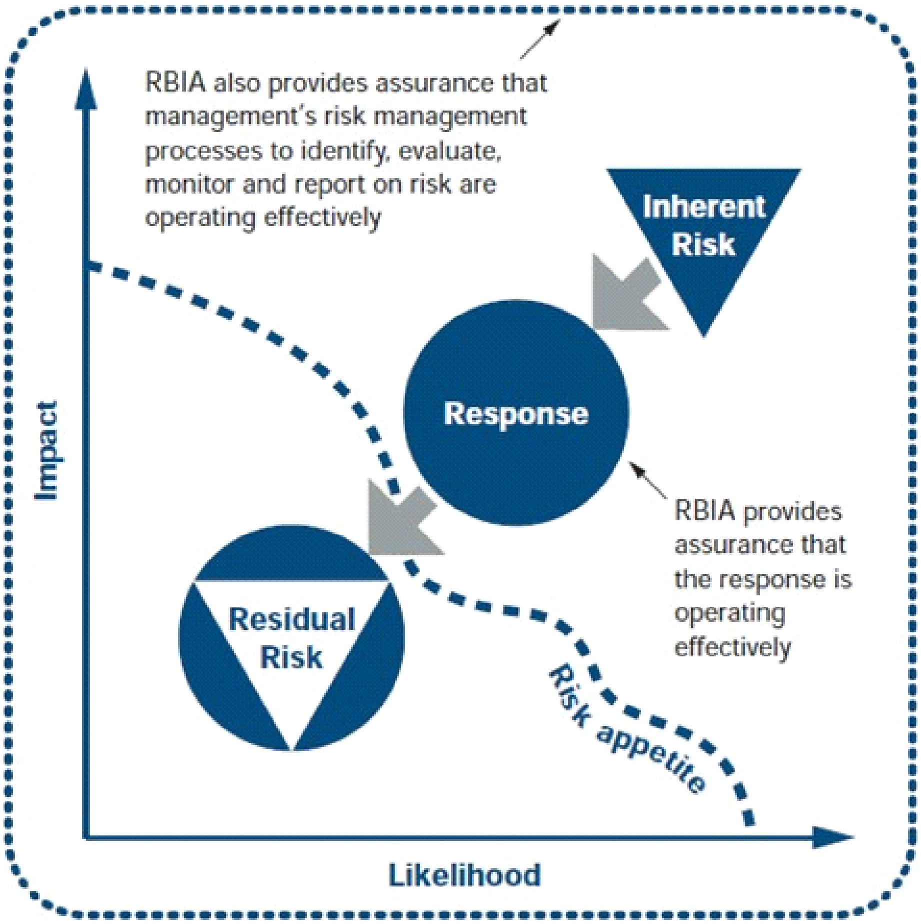
Production of the audit plan

Chartered Institute of Internal Auditors

RBIA is not about auditing risks but about auditing the management of risk. Its focus is on the processes applied by the management team:

- The responses to individual risks, and
- The processes used to assess risks, to decide on the responses to them, to monitor the responses and to report to the board.

Presentation of assurance provided by RBIA:


RBIA also provides assurance that management's risk management processes to identify, evaluate, monitor and report on risk are operating effectively
Inherent Risk
Response
RBIA provides assurance that the response is operating effectively
Residual Risk
Risk appetite
Impact
Likelihood

Expand this diagram

Objectives of this stage

The objectives of this stage are to:

1. Agree all the risk management responses and risk management processes on which objective assurance from internal audit is required
2. Produce an audit plan which lists all audits to be carried out over a specified period - usually a year.

Information requirements

Stage 1 should have provided the background needed to understand how management identifies and evaluates risks and how and where the rest of the information needed is recorded.

The risk register, or attached documents, show responses, actions and monitoring controls:

- the responses that management believe exist to manage key risks
- the actions that are being taken to add, delete or modify existing responses where they do not currently bring risk within the risk appetite
- the monitoring controls used by management to ensure that all these elements of the framework are working.

Internal audit should also obtain from the audit committee and the management team guidance about the nature of the objective assurance they want from the internal audit activity. These are called the assurance requirements. They may be explained in a separate document or as part of the risk register, or they may be identified as a result of discussions with the people involved.

In RBIA the role of internal audit is not to create any of this information but to be able to interpret it and to use it for planning purposes.

Actions to achieve the objectives

The steps to complete Stage 2 are shown as follows.

1. Identify the responses and risk management processes on which objective assurance is required.

Internal audit should review the audit committee's assurance requirements and the risk register and list all the responses on which objective assurance is required, together with information on the risks to which they are related.

Reponse to risk	Processes to audit
Terminate activities if the risks they pose are too high or too costly	Action plans and projects to terminate he activity

Tolerate a risk	Monitoring the risk
Transfer a risk	Processes for transferring risks
Treat a risk	These include the familiar accounting and operational controlsthat have been the focus of internal audit for many years

Other risk management processes on which assurance may be required include:

- Action plans to increase or reduce the amount of transfer or treat responses; and
- Monitoring controls to ensure that the processes and action plans are operating as expected.

Internal audit should provide assurance on parts of the risk management framework itself:

- processes used to identify and assess risks and to decide on the appropriate responses, and
- processes for reporting risks throughout the organisation; and monitoring controls over those processes.

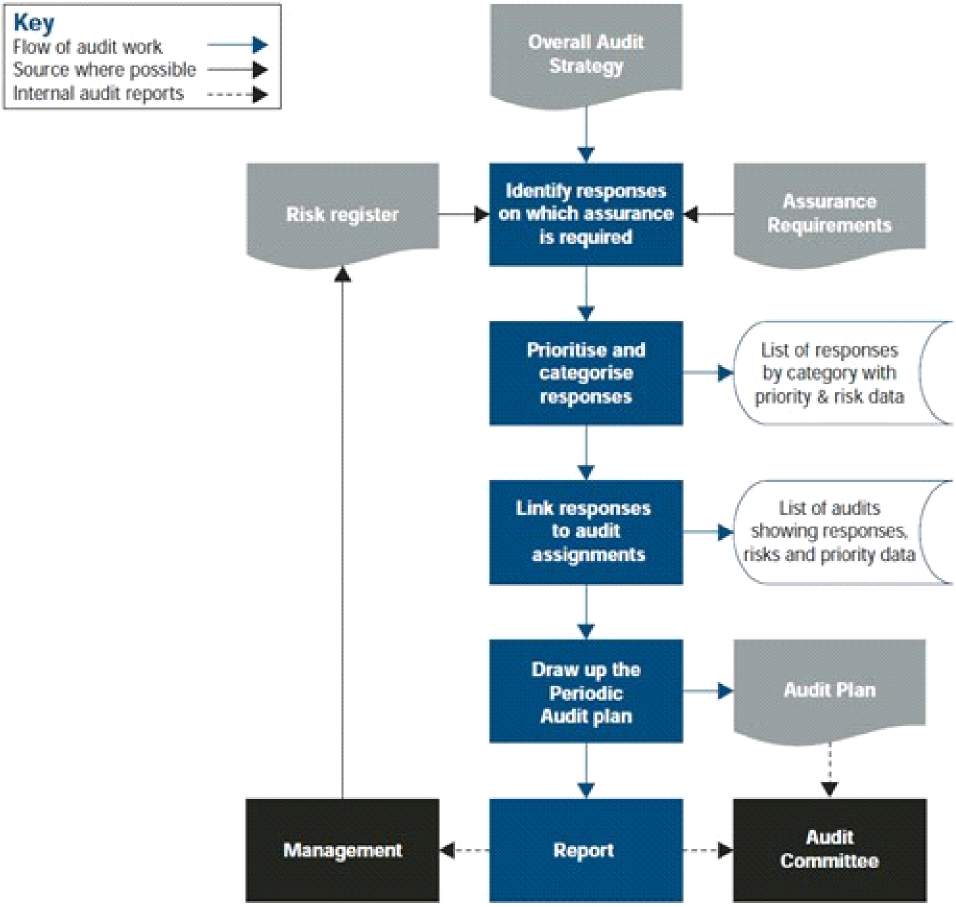
The audit committee may not want objective assurance from internal audit on the management of all the risks. Reasons not to want such assurance may include:

- the quantity of assurance from other sources
- the skills and competence of the internal audit activity in a specialist area
- the availability of objective assurance from other sources.

The audit committee may prioritise the risks on the management of which it would like objective assurance, favouring higher inherent risks. It may not, therefore, require objective assurance on all risks every year.

Internal audit may wish to review thoroughly the audit committee's assurance requirements to ensure that they do not leave a gap in assurance. It is important to recognise that the internal audit activity does not have to provide assurance on every aspect of the risk management framework in order for it to be effective.

Producing the audit plan:


Key
Flow of audit work
Source where possible
Internal audit reports
Overall Audit Strategy
Risk register
Identify responses on which assurance is required
Assurance Requirements
Prioritise and categorise responses
List of responses by category with priority & risk data
Link responses to audit assignments
List of audits showing responses, risks and priority data
Draw up the Periodic Audit plan
Audit Plan
Management
Report
Audit Committee

Expand this diagram

2. Categorise and prioritise the risks.

If there is a large number of risks, they should be categorised. This should result in grouping the risks into a logical order, which will help in compiling the audit plan. Useful categorisations include:

- By business unit. This is useful where the organisation has a number of physically independent business units, the procedures and systems of which are self-contained. It may be necessary to duplicate common responses, for example, those arising from computers, across all units.
- By function or system, such as sales, purchases, or stock control. This is useful in a large central organisation with integrated systems.
- By objectives. This is useful when assessing the audit plan for its relevance to the organisation because it links audits directly to the objectives affected by the risks, the management of which is being checked by the audit.

Internal audit should also prioritise the responses which are to be audited. An important characteristic of RBIA is that prioritisation is always by reference to the size of the risks and to the contribution that the response makes to managing the risks. Useful prioritisations include:

- The size of the inherent risks managed by the response: the bigger the risk, the higher the priority.
- The contribution that the response makes in managing risks so that the more the response reduces the risk, the higher the priority. For example, where a risk is managed using a single response, say a treatment, the control score - (the difference between the inherent risk and the residual risk) - is the contribution of that response. However, the control score for some risks may be divided among different responses, which needs to be taken into account.
- The number and nature of other available assurances that the response is operating effectively. Where several groups provide assurance on a single response, it may have a lower priority.
- Those categories of risks on which the audit committee requires objective assurance each period.

3. Link risks to audit assignments.

Two methods can be used to link risks to audit assignments:

1. Group the risks, for example by business unit, objective, function or system, and decide the audits which will provide assurance on the related responses.

   This method has the advantage that the management of all risks will be covered, but it may be difficult to define audit units which satisfy the organisation's preferences for audit size", such as the number of staff hours on an audit.

2. Set up an audit universe.

   This allocates each audit to a business unit or system and assigns the risks, on which assurance is to be provided to these audits. This method has the advantage of covering one physical location in one visit and of allowing the definition of suitably sized audit units. It requires an additional check to ensure that the management of all risks is being audited.

This step will produce a list of potential audit assignments. The priority of each audit is derived from the size of the risk management process on which it provides assurance. This information should link to the categorised listing of risks, which in turn links to the risks in the organisation's risk register.

The organisation also needs to collect and record information that links the risks, the responses to them and the audit assignments which provide assurance on those responses.

An example can be found in Appendix E: Risk & audit universe (part), the risk and audit universe, which may either be a separate document or form part of the risk register.

4. Draw up the periodic audit plan.

Estimate the number of days required for each audit and identify which audits can be completed with the available resources, while providing scope for consulting support.

RBIA generates a defined amount of work and, therefore, highlights whether resources are sufficient to complete the planned work. Internal audit can propose an increase in staff, or a reduction in the number of audits if there are insufficient resources.

Management and the audit committee should be informed of any risks on which assurance will not be provided.

All the audits to be included in the plan should have now been determined. However, many organisations add audits based on criteria other than risk. Such criteria might include areas subject to change, mandatory audits or audits requested by management.

This is a reason to 'sense check' the RBIA work so far because any topic worthy of audit should have surfaced through the risk management framework.

For example, considerable change happening in an area could result in increases in the likelihood of a risk event materialising and this should be visible in the risk register.

If an audit has to be included by management request, then it is displacing an audit included on the basis of risk scores and management should justify this substitution.

5. Reporting to management and the audit committee.

The periodic audit plan should be discussed with management and be presented to the audit committee for approval. It should provide:

- Details of those risks where assurance is provided by carrying out the audits of the risk management processes and responses in the plan.
- Details of those risks where assurance is provided but based on audit work from previous years, if applicable.
- Details of those risks where consultancy work is carried out to assist management in reducing the risks to below the risk appetite, or, at least, an indication of the resources available for consultancy work.
- The impact of any constraints on resources.
- Any risks not covered due to policy constraints.
- Confirmation that the plan is in accordance with the internal audit activity 's terms of reference.

Appendix F: Audit plan (April 2005 - March 2006) provides an example.

Internal audit should report to management any information that has come to light about the quality of the risk register. If extra topics for audit have been identified at the end of Stage 2 these should be discussed with management so that management can revise the risk register.

Risk defined organisations starting to use RBIA

If an organisation is risk defined it does not have a complete risk register. Internal audit should use completed parts of the risk register to plan, or re-plan, audit work using the method above.

For those parts of the organisation without a complete risk register, internal audit should use an alternative framework as discussed under 'Range of audit strategies' in Risk maturity assessment.

Next: Doing the audit

Appendices

Guidance on implementing key aspects of RBIA methodology:

A: Assessing the organisation's risk maturity

Illustrations of how you might document parts of the risk management framework and RBIA:

29 May 2014

Doing the audit

Chartered Institute of Internal Auditors

Since RBIA is not about auditing risks but about auditing the management of risk, it focuses on the actions taken by the management team to respond to risks.

Internal auditors need to spend time with managers, discussing and observing the monitoring controls they apply, rather than re-performing controls or other responses, or analysing data for themselves.

Internal auditors should behave in a way that reinforces the fundamental principle that management is responsible for managing risks. Procedures should exist to enable internal auditors to report issues to management and agree with them the action they will take to update the risk register.

Objectives of this stage

To provide assurance that, in relation to the business, activity, or system under review and for the processes identified in the audit plan:

- Management has identified, assessed and responded to risks above and below the risk appetite.
- The responses to risks are effective but not excessive in managing inherent risks within the risk appetite.
- Where residual risks are not in line with the risk appetite, action is being taken to remedy that.
- Risk management processes, including the effectiveness of responses and the completion of actions, are being monitored by management to ensure they continue to operate effectively.
- Risks, responses and actions are being properly classified and reported.

Action to achieve these objectives

The steps to complete this stage are:

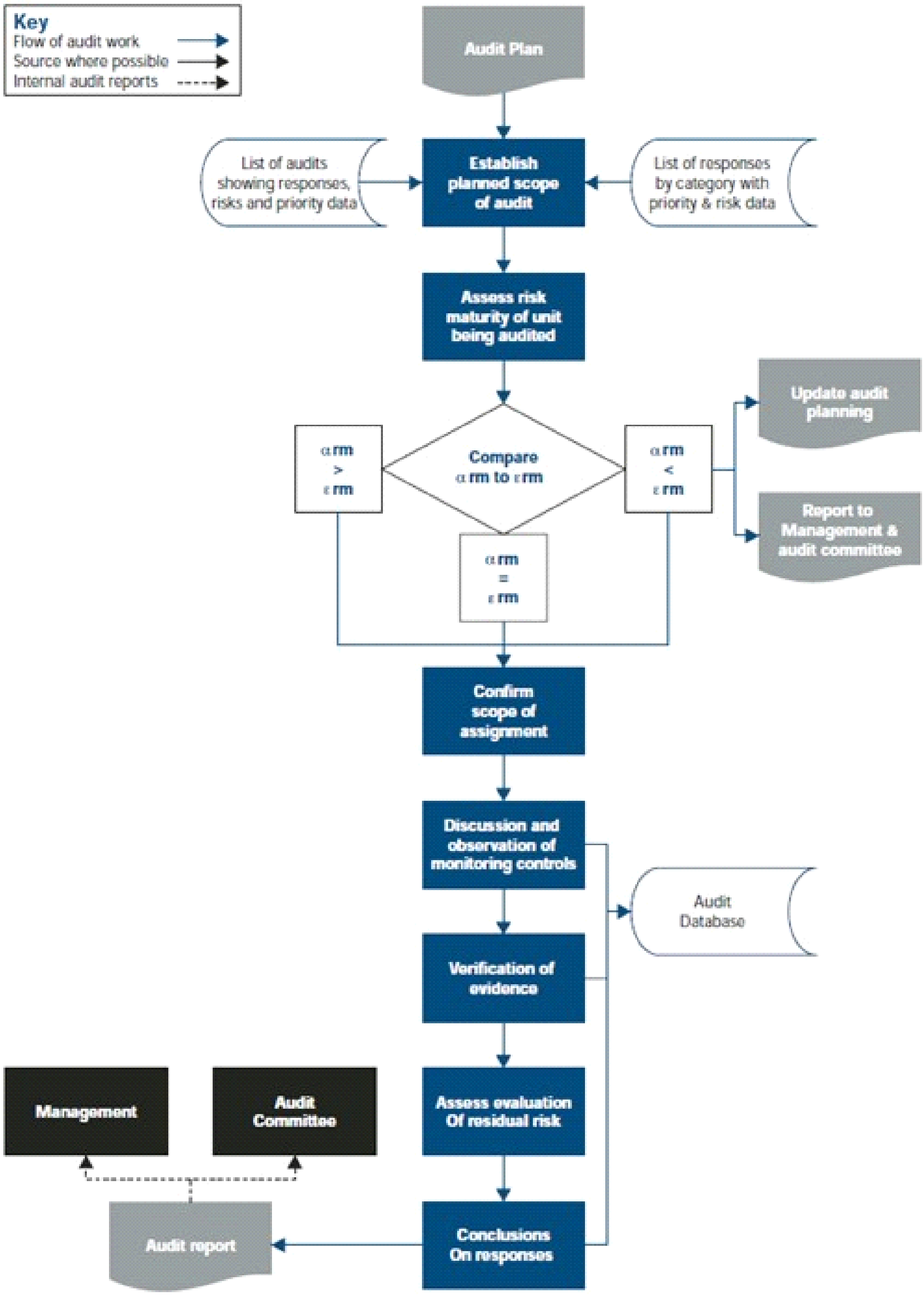
1. Establishing the planned scope of the assignment.

This involves the internal auditors understanding the results of Stages 1 and 2 in order to draw up the draft scope. Relevant information includes the conclusion on the risk maturity and the resulting audit strategy, the title of the assignment and information that links the audit to the responses on which it should provide assurance and then to the risks managed by the responses.

2. Assessing the risk maturity of the unit being audited.

This allows internal audit to take its assessment to a more detailed level than was possible at Stage 1. The criteria used to assess risk maturity should be consistent with those used in Stage 1 and in other assignments. The assignment may include scrutiny of the risks identified by management, which may need additional or expert resources.

Performing the audit:


Key
Flow of audit work
Source where possible
Internal audit reports
Audit Plan
List of audits showing responses, risks and priority data
Establish planned scope of audit
List of responses by category with priority & risk data
Assess risk maturity of unit being audited
Compare α rm to ε rm
α rm > ε rm
α rm = ε rm
α rm < ε rm
Update audit planning
Report to Management & audit committee
Confirm scope of assignment
Discussion and observation of monitoring controls
Audit Database
Verification of evidence
Management
Audit Committee
Assess evaluation Of residual risk
Audit report
Conclusions On responses

Expand this diagram

3. Assignment-level conclusions on risk maturity.

Conclusions from individual audits should either confirm or cast doubt on the original organisation-level assessment. This initial assessment may need to be changed.

If the actual risk maturity (arm) is better than or the same as the expected risk maturity (erm), the current assignment will carry on as planned.

If arm is lower than erm, internal audit should report this to management, together with the conclusion that responses included in the audit scope are not working effectively.

This may be the end of the audit assignment or, if the nature of the shortfall in risk maturity means that some responses may still be effective, the scope of the audit may be restricted to those responses only.

4. Confirming the scope of the assignment.

Under RBIA, internal auditors need more of management's time than they would in other approaches to internal audit. Heads of internal audit may wish to support the audit team by marketing the approach and gaining buy-in from the management prior to conducting audit work.

5. Discussion and observation of monitoring controls.

This is the first stage of the audit testing. The aim is to determine that the controls used by management to ensure that the risk management framework is working are designed to achieve this objective and to show that they are working as designed.

6. Verification of evidence, walkthroughs, re-performance, etc.

These activities may also be required to provide extra evidence that responses to key risks are working effectively and to support a conclusion that the monitoring controls are also working.

7. Documenting the results of the audit work.

This differs in RBIA from standard practices mainly in that the link between risks, responses to risks, assurances given and work done to support those assurances has to be made clear.

8. Assessing management's evaluation of residual risks.

This produces a conclusion about specific scores in the risk register and should lead to findings about how management determine residual risks in general. If there is a systemic failing, internal audit should ensure that it is reflected in the organisation-level conclusions on risk maturity.

9. Conclusions on responses and risk management processes covered by the assignment.

This covers both their design and how well they are working. The conclusions need to be linked to the risks that are managed by the responses so that the assignment can deliver the assurances that are the aims of this stage. One suggested way to draw the conclusions is given in Appendix B: Guidance on assigning audit conclusions. This should be tailored to individual needs.

10. Reporting and feedback.

This should be in accordance with the organisation's policies, including whatever levels of review are required by audit management.

This step is critical to your aim of reinforcing management's responsibility for managing risks. Findings should be discussed with management in such a way that they take responsibility for deciding on appropriate remedial actions, including all and any changes to the risk register.

If this is a big change in the style of the internal audit activity, the effort required to implement it properly should not be underestimated. Internal audit may need to play a bigger role in drafting and delivering reports for the first months of implementing RBIA.

To complete the RBIA steps and stages the findings from individual assignments are fed back into the overview of the organisation begun in Stage 1 because:

- The findings may change the conclusions on risk maturity and may need to be reflected throughout the audit plan the next time it is updated.
- The findings need to be reflected in the reporting of risks so that management and the audit committee understand where objective assurance has been provided.

11. Summarising the audit conclusions for the audit committee.

This summary should:

- Support the requirement of any regulations which apply to the organisation.
- Fulfil the requirements of the audit charter.
- If not part of the charter, provide an opinion on whether risks are being managed sufficiently to ensure the organisation's objectives are being achieved and, within reasonable limits, will be achieved in the future.

Repeating the cycle of RBIA

The RBIA methodology is cyclical. The interval between revisions in internal audit's assessment of the risk maturity and its audit planning depends on the nature of the organisation: how often its circumstances change and how frequently it must report on risk management matters. The interval should be agreed with the audit committee.

Changes to the assessment of risk maturity may change the audit strategy. Changes to the risk register, arising from changes to the assessment of risks or from changes in the responses to risks, may change which responses require auditing, the way they are allocated to audit assignments and the priority of the different audits.

Other sources of change include:

- audit work
- the risk management framework
- the external environment
- the objectives of the organisation.

Audit work gathers evidence on the risk maturity of the organisation which is fed back into the assessment.

The risk management framework is a dynamic construction, dependent on people to operate effectively, and it takes continuous effort to keep it working well.

As the external environment and the objectives of the organisation change, the circumstances and context of potential risk events also change so that the risk register needs to evolve as time passes.

Next: Benefits and drawbacks of RBIA

Appendices

Guidance on implementing key aspects of RBIA methodology:

Illustrations of how you might document parts of the risk management framework and RBIA:

29 May 2014

Benefits and drawbacks

Chartered Institute of Internal Auditors

RBIA is inextricably linked to the risk management framework. During Stage 1 it allows a conclusion on the risk maturity of the organisation. If this is not high, it provides internal audit with an opportunity to report that fact promptly to management and the audit committee so that they can take immediate action.

While this allows the internal audit activity to provide value to its organisation, RBIA is a challenging prospect. Organisations with a poor level of risk maturity may be that way because the managers and directors do not accept that a good risk management framework is an essential element of a sound system of internal control.

Internal audit may need to undertake a longer term programme of activity to champion risk management.

Direct contribution to the organisation's objectives

An effective risk management framework will improve an organisation's governance and its chances of achieving its objectives over the long term.

The RBIA methodology makes a clear and valuable contribution to the risk management framework by providing objective assurance and by facilitating management's efforts to improve the framework.

It ensures that internal audit resources are directed towards assessing the management of the most significant risks.

Relationship with management

The RBIA approach requires increased management involvement.

Since the processes to be covered in audits exist in all parts of the organisation, audits may involve managers in departments never before visited.

In order to discuss the responses deployed to manage risks and how management knows these are working properly the internal auditor may need to involve a greater number of more senior managers than might be involved in traditional audits.

RBIA emphasises management's responsibility for managing risks. This must be stressed during all meetings with managers.

The close-down meeting is less about management accepting internal audit's recommendations and more about management agreeing that an issue exists and determining what action it is going to take and what reporting it needs to provide to the next level of management.

As a result, the head of internal audit may be required to market the benefits and the need for internal audit. A much higher profile may be necessary in non-financial areas in order to pave the way for audits that managers can understand and support. The implications for staff expertise are discussed overleaf.

Management responsibility for risk management

RBIA can be implemented fully only in risk enabled and risk managed organisations. One characteristic of this level of risk maturity is that managers have to take responsibility for managing risks. In taking responsibility for risks, managers understand that controls, like other responses to risks, are not the responsibility of internal audit, imposed by internal audit, but are their own responsibility.

Implementing RBIA means that the internal audit activity behaves in a way that reinforces this management responsibility and thus contributes to a stronger risk management culture.

Achieving targets

RBIA is an effective way to achieve targets set for the internal audit activity, such as:

- The compilation of an audit plan which ensures the internal audit activity fulfils its charter
- Gaining acceptance from management that it takes appropriate action to manage risks within the risk appetite;
- Provision of objective assurance in the three areas of risk management normally required; and
- Keeping within the budget set for the activity.

Audit resources

RBIA justifies the number of auditors required. The audit plan, including the resources required, is driven by the proportion of processes and risks on which the audit committee requires objective assurance.

This differs from alternative approaches, where the resources available determine the audits which can be carried out.

Staff expertise

Internal auditors engaged in RBIA require more people and business skills, such as interviewing, influencing, facilitating and problem solving.

The expansion of the audit universe to cover all risks threatening the organisation's objectives requires the internal auditor to conclude on the design and operation of responses to risks in areas that may be new.

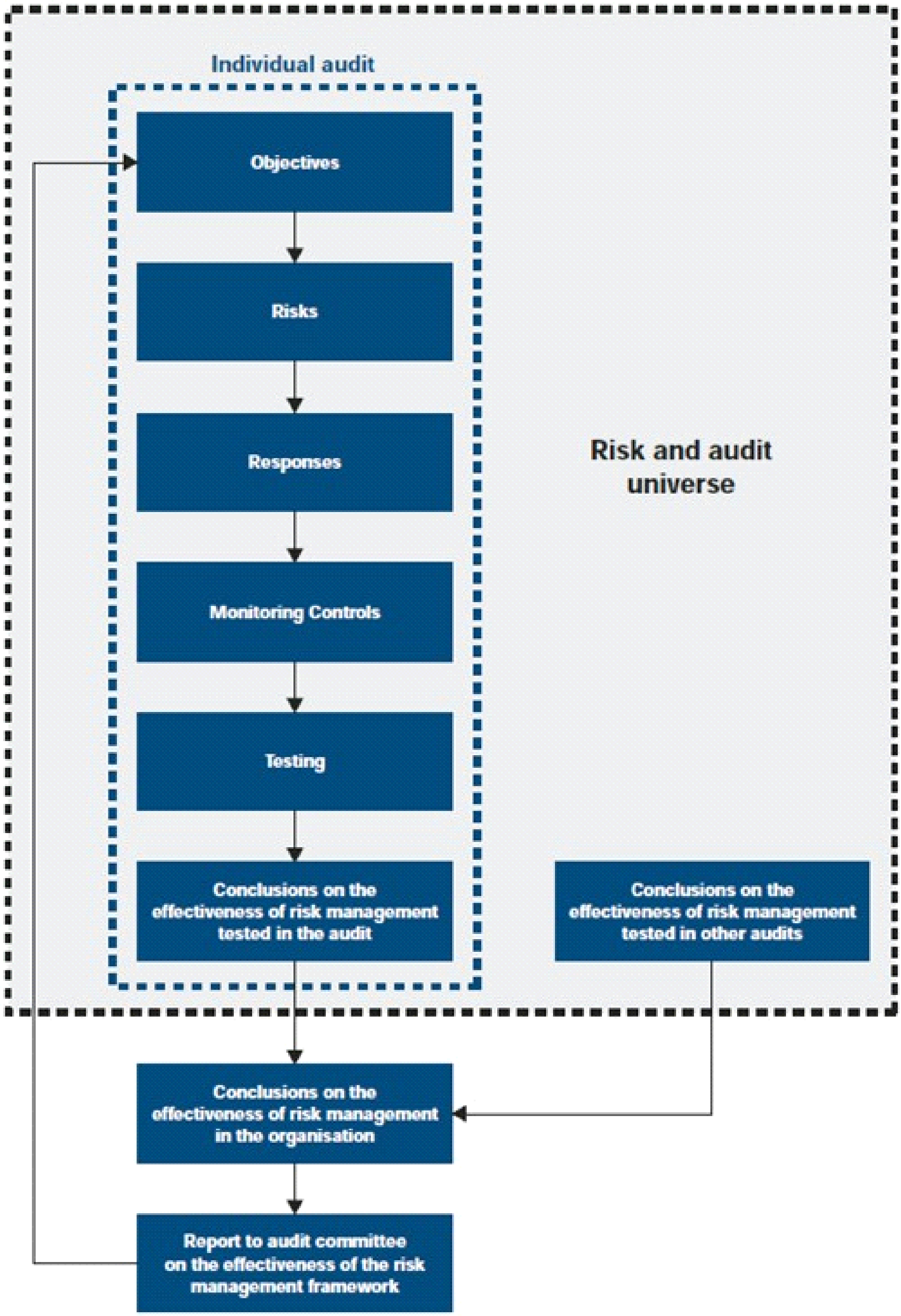
This may require specialist knowledge that may be acquired as follows:

- Use specialist skills already available within the internal audit activity, e.g. computer auditors.
- Provide specialist training to auditors with general expertise, e.g. provide training on the regulations and practices related to stress management to an auditor who already a holds an Advanced Diploma in Internal Auditing and Management.
- Recruit temporary or permanent specialists from inside the organisation, e.g. a warehouse manager from one overseas subsidiary could audit warehouse processes in another.
- Use specialists from outside the organisation, e.g. treasury specialists.

An audit trail for audits

RBIA ties all aspects of internal auditing together: objectives, risks, processes for responses and monitoring controls, tests and reports, as shown on the diagram below.

RBIA - An audit trail:


Individual audit
Objectives
Risks
Responses
Monitoring Controls
Testing
Conclusions on the effectiveness of risk management tested in the audit
Risk and audit universe
Conclusions on the effectiveness of risk management tested in other audits
Conclusions on the effectiveness of risk management in the organisation
Report to audit committee on the effectiveness of the risk management framework

Expand this diagram

The relevance of any test can be seen in relation to the opinion on the entire risk management framework because of the relationships set up in the risk and audit universe.

RBIA provides an audit trail from an individual audit report back through tests, processes and risks to objectives, and forward to the audit committee report on whether those objectives are threatened.

Webinar on RBIA

Stephen Maycock talks about how RBIA might be applied within a range of internal audit processes in our free webinar