

Risk Appetite & Assurance  
Do you know your limits?



# Contents

---

1. Effective risk appetite	1
2. Considerations for Internal Audit's assurance approach	3
3. Benefits of effective risk appetite frameworks for Internal Audit	5
4. Concluding thoughts	6
Contacts	7

---

# 1. Effective risk appetite

UK, other European Supervisory bodies and the global regulatory community are building an emerging consensus on what constitutes an effective risk appetite framework. The Financial Stability Board has released a consultation paper on the subject: *Principles for an Effective Risk Appetite Framework* and understanding whether the organisation has a fit for purpose framework that accords with these principles is firmly on Board agendas.

Internal Audit should assist the Board by providing independent assurance over the design and effectiveness of the risk appetite framework. This will involve an assessment of both its alignment with supervisory expectations (design) and extent to which it has been embedded in the business (operating effectiveness).

The need for an effective risk appetite framework was reinforced through observations of failures in its absence during the financial crisis.

Regulatory guidance across Europe has focussed on delivering “greater clarity and an elevated level of consistency among national authorities”.<sup>1</sup> It is therefore helpful to establish a common language within and between organisations and regulators when discussing this subject.

## Components

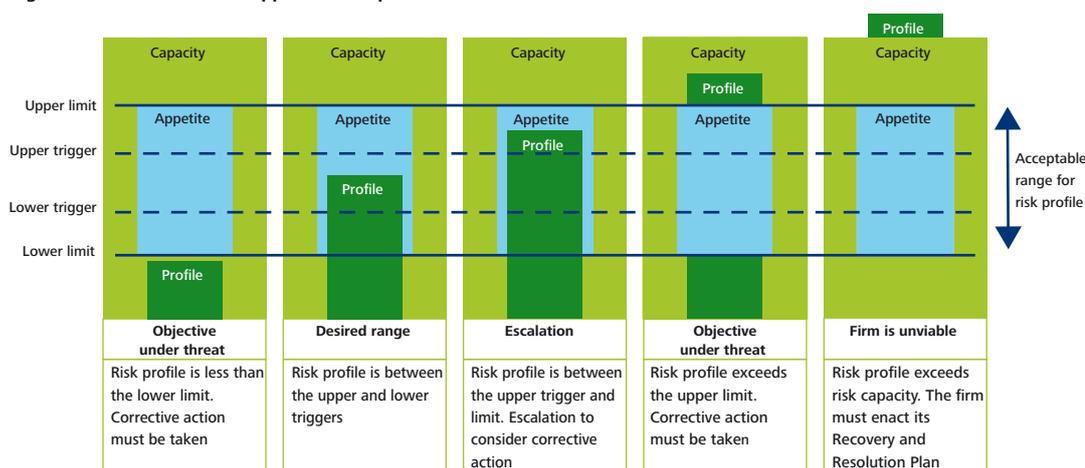
An effective risk appetite framework combines a series of appetite statements, limits, measures and standards that together enable the Board and the business to set, monitor and manage:

- Risk appetite.<sup>2</sup>
- Risk capacity.<sup>3</sup>
- Risk profile.<sup>4</sup>
- Risk appetite limit.<sup>5</sup>
- Risk appetite triggers.<sup>6</sup>

Effective design of a risk appetite framework demands a clear understanding of the relationships between these concepts, expressed graphically in Figure 1 (below).

- 1 Principles for an Effective Risk Appetite Framework, Financial Stability Board, November 2013
- 2 The risk a firm is willing to take in the pursuit of its strategy.
- 3 The maximum level of risk at which a firm can operate, while remaining within the constraints implied by capital and funding needs and its obligations to stakeholders.
- 4 The firm’s entire risk landscape reflecting the nature and scale of its risk exposures aggregated within and across each relevant risk category.
- 5 The level of which, if breached by the firm’s risk profile, would necessitate immediate escalation and corrective action.
- 6 The level at which escalation occurs to a higher forum, committee or level of authority because the risk profile is sufficiently close to the risk appetite limit that corrective action should be considered.

Figure 1. Interaction of risk appetite concepts



---

## Effective risk appetite frameworks have both depth, required to be meaningful to the business, and breadth, so as to encapsulate the full risk spectrum of the organisation.

### Characteristics

Effective risk appetite frameworks have both *depth*, required to be meaningful to the business, and *breadth*, so as to encapsulate the full risk spectrum of the organisation.

1. **Depth:** the framework should support execution of the firm's business strategy and therefore be capable of expressing appetite at the aggregate level. However, its design and operation must reach the granular levels at which risk is taken in the business so that it is an effective tool to manage risk, and not simply a grand statement that has no impact on risk takers in their day to day activities. Depth in this sense will involve a hierarchy of delegated authorities and activities.
2. **Breadth:** the framework must encapsulate the full risk universe of the organisation. Breadth in this sense will involve defining the significant risk exposures (financial and non-financial) of the organisation's activities as well as the measures (quantitative and qualitative) that can be incorporated in the framework.

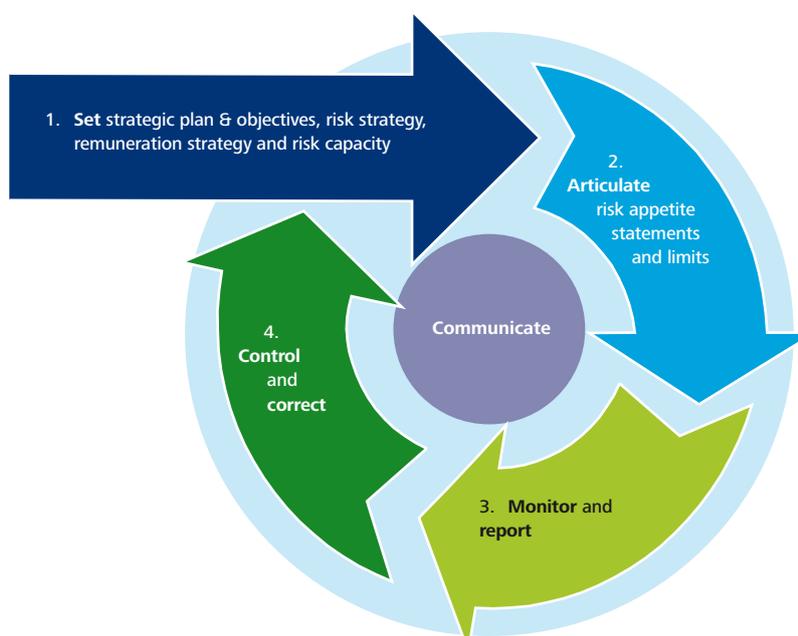
### Implementation & use

There should be policies and processes in place to:

- set the strategic plan and objectives as well as the risk strategy and understanding of ultimate risk capacity;
- set, articulate and cascade risk appetite statements and associated limits;
- monitor and report risk profile versus appetite and triggers; and
- manage the risk profile.

This should be a dynamic process, as depicted in Figure 2, with appetite and limits responding to the business environment and/or changes to risk capacity as required. Achieving this dynamism, and the breadth and depth discussed earlier, is greatly assisted by the use of a common organisational language with respect to the components of the framework.

Figure 2. The risk appetite cycle



## 2. Considerations for Internal Audit's assurance approach

Recent regulatory guidance<sup>7</sup> has outlined a clear set of roles and responsibilities across the business including those of the: Board; CEO; CRO; CFO; BU leaders; and Internal Audit.

Internal Audit must deliver assurance on both the design of the risk appetite framework and its operating effectiveness. A properly functioning risk appetite framework contains key components at all levels of the business, and business level activity is not solely operationalising of Board level risk appetite activity. Therefore Internal Audit should ensure it carries appropriate testing in all parts of the business.

### Design and implementation

Internal Audit should, as a third line of defence, provide assurance to the Board on the risk and control environment of the organisation, encapsulating risk management activity performed by the business, as well as the oversight and assurance framework provided by the second line. Risk appetite is a concept which both underpins, and is crucial to, an effective risk and control framework. Internal Audit's focus should therefore be around the extent that the risk appetite framework is effective and robust so that it can aide, support and drive an effective risk and control environment.

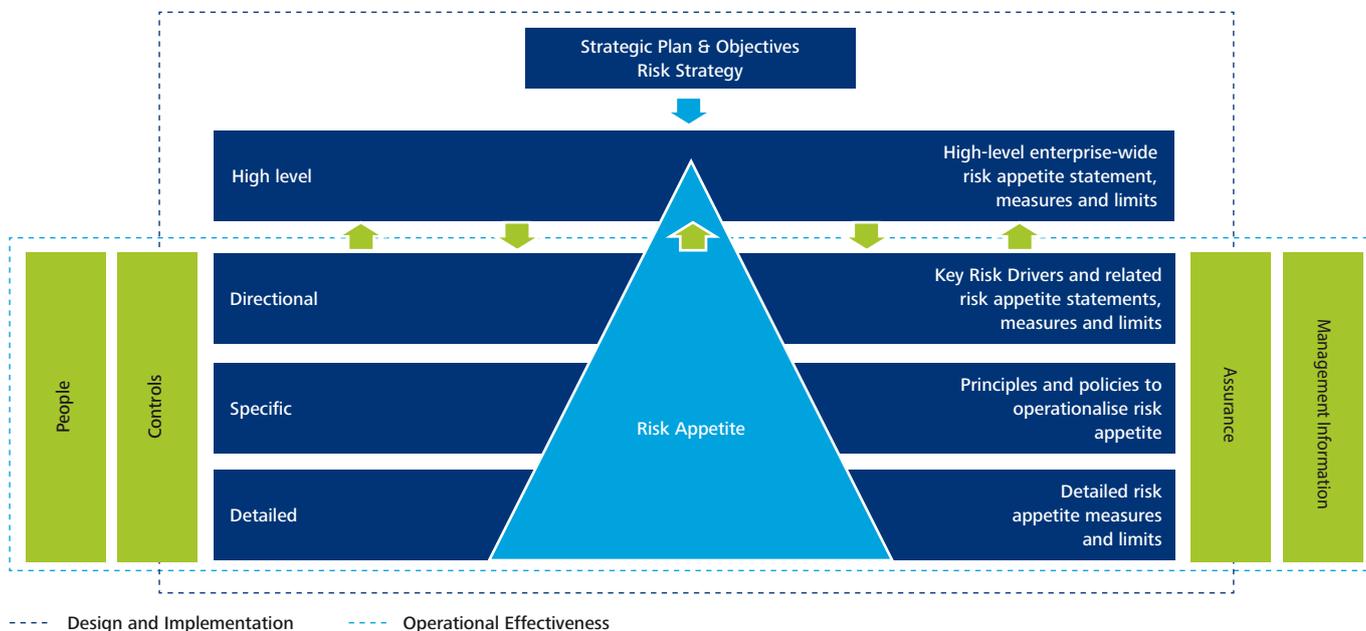
**Strategy** – The risk appetite framework should articulate the level of risk that the Board is willing to take in pursuit of its strategy. Internal Audit should assess the extent that risk appetite statements within the firm align to the strategic mission statements of the business. With a fully effective framework, evidence that the firm is consistently operating outside of appetite indicates it is not managing to effectively execute the strategy. Conversely the framework may not be fully effective, for example risk appetite limits may be set too low to enable the business to achieve its goals. Overall, strategy and appetite must reconcile. The risk appetite framework should support and inform business performance.

**Scope and qualitative measures** – Internal Audit should assess whether risk appetite is considered for the entire risk universe of the business. In doing so it should evaluate how well the framework incorporates and articulates non-quantitative risk exposures such as conduct-related, ethical or reputational risks. These can be difficult to measure, in comparison to quantitative metrics such as capital and liquidity ratios. An effective risk appetite framework should be able to articulate and aggregate appetite measures across all risk types that the business is exposed to.

**Ownership** – As with other risk framework components, the second line should provide the framework, tools and standards through which risk appetite should be set and managed. The first line and senior management should be responsible for setting the appetite and making associated decisions (e.g. monitoring) that may be performed by the first or second lines. Internal Audit should seek to establish how clearly defined ownership of the framework and subsequent responsibilities are, in addition to testing that those responsibilities are delegated appropriately.

**Governance and Management Information** – Remediation plans should be clear and consistent across all appetite measures to ensure the overall appetite aggregation is accurate and appropriate, and tracked accordingly within the existing risk governance framework. There should be defined responsibilities and delegated authorities within the governance structure if risk appetite is to ensure clear accountability and transparency around decisions made. Triggers and limits should be appropriately managed, and amendments controlled.

Management Information should be appropriately aggregated as it is escalated but still accurately reflect appetite statements and detailed risk appetite measures and limits. Any limitations in Management Information, through aggregation or data quality, should be appropriately acknowledged to ensure informed decisions.



### Operational Effectiveness

Internal Audit may be able to provide even greater assurance and add value to the overall quality of the framework by conducting deep-dive reviews on particular granular aspects, for example:

**Risk measures** – Internal Audit could review the population of risk measures, which should be catalogued in a risk register, and assess their completeness and degree of linkage to the risk appetite.

**Policy and process framework** – Many organisations see benefits from operationalising their risk appetite in the form of minimum policy standards and assessing compliance against these standards.

**Management Information** – Internal Audit may review in detail the way in which decision makers are presented with MI relating to the risk appetite of the business. They may question the prominence of certain measures, the level of aggregation or disaggregation, the timeliness of the measures, any limitations in the data and the periodicity of the reporting.

**Assurance** – How well is appetite reflected in other assurance functions? Are first or second line providing assurance on areas which are not part of risk appetite? If so, what decisions are made around this? i.e. Does the assurance add any value to the organisation, or more crucially, are there areas of the business where assurance is conducted which is not reflected in risk appetite? This would suggest signs of a lack of embedding.

**Policies** – How well is risk appetite reflected in business policies? Management should have an understanding of risk appetite and the impact it has on their areas, in order to ensure the staff in their area conduct processes within appetite. This is demonstrable by building appetite style behaviour into policies to ensure staff are aware of processes which may fall outside of risk appetite, and are able to identify, report and escalate this, albeit not necessarily using technical language. A lack of articulation and embedding of appetite at this level (through, for example, business policies such as Change Management, Information Security, Investment etc.) could result in a lack of understanding by staff. This can then cause ineffective management of risk appetite, including the ability to measure, monitor, report and escalate.

**Culture and embedding** – Internal Audit should be cognisant of any activity within the business which would illustrate how well risk appetite understanding and management is embedded within the business. This is evident by the acknowledgement of appetite, or the impact activity may have on appetite, through key decision making such as new product approval processes or operational changes.

# 3. Benefits of effective risk appetite frameworks for Internal Audit

There are significant potential benefits available to Internal Audit where the organisation has embedded a comprehensive risk appetite framework. Subject to the caveat that the framework has been evaluated in terms of design and operating effectiveness (and found to be adequate), Internal Audit functions may choose to make use of available Management Information outputs to inform their other assurance activities.

Once Internal Audit has satisfied itself as to the design and effectiveness of the risk appetite framework it may consider the assurance activity performed in the first and second lines. To the extent that this is robust, and subject to periodic assessment by Internal Audit, this may allow Internal Audit to focus its attention elsewhere.

## Risk focused prioritisation

If the risk appetite framework has mapped all the activities of the organisation that give rise to risk – a pre-requisite to effectively determining its scope – then this becomes a helpful reference for Internal Audit, who may then compare its own audit universe to the risk universe. Where there are risks present in the audit universe that are not recognised by the risk appetite framework, there are two possible conclusions to be drawn with associated remediative activities:

1. The risk appetite framework is not comprehensive – this area of business activity should be brought within the scope of the framework.
2. The 'risk' identified is insignificant in the context of the organisation's overall risk profile, i.e. there has been a deliberate and valid 'de-scoping' of these activities from the framework's scope – in such a case it would appear to be an inefficient use of third line resources to devote time to this set of activities.

Equally, Management Information from the risk appetite framework may offer Internal Audit valuable data points to drive prioritisation of assurance activity. For example, Internal Audit could utilise data from breaches of risk appetite triggers, or changing risk appetite limits to make quicker and more dynamic decisions on those business activities that they plan to assess.

## Acknowledge limitations

As with all areas of Internal Audit, it is imperative that assurance teams have the skills, knowledge and experience to produce robust assessments. Given that risk appetite is an emerging and constantly developing area of the risk discipline, this may not exist within in-house teams. Consideration should be given to supplementing in-house auditing skills with externally sourced subject matter expertise if this is the case.

Further, the scope of the risk appetite framework may identify sources of risk that have not previously been subject to assessment by Internal Audit. Again, where these are highly specialist in nature, this may lead Internal Audit functions to conclude that they require assistance in formulating and/or delivering an assurance plan in these areas.

Internal Audit should also consider the degree to which they are able to leverage the risk appetite framework due to limitations in the underpinning technology and infrastructure on which it is built. Immature capability in analytics, data extraction and report generation can make the audit process inefficient.

---

**The scope of the risk appetite framework may identify sources of risk that have not previously been subject to assessment by Internal Audit.**

## 4. Concluding thoughts

There are four key takeaway points we feel Internal Audit should consider in both how they assess risk appetite, and how they may utilise it:

	<p>Boards need to ensure the quality and effectiveness of risk appetite frameworks as a priority, as they will be subject to regulatory scrutiny.</p>
	<p>Internal Audit should move to deliver assurance to the Board on the control framework by reference to a firm's ability to manage activity within risk appetite.</p>
	<p>Internal Audit actions should seek to drive a comprehensive and fully embedded risk appetite framework so Internal Audit functions can then adjust their broader assurance plans based on the intelligence provided by monitoring performed within the framework, maximising assurance effectiveness.</p>
	<p>Risk appetite is still evolving, and for some firms, is a complex topic. Internal Audit functions should consider any limitations in resource and ability when developing their approach to both assessing and utilising their organisation's risk appetite framework.</p>

# Contacts

## UK Financial Services Internal Audit Leadership Team

**Mark FitzPatrick**  
*Vice Chairman and Partner*  
+44 (0) 20 7303 5167  
mfitzpatrick@deloitte.co.uk

**Paul Day**  
*Partner, Banking and Capital Markets*  
+44 (0) 20 7007 5064  
pauday@deloitte.co.uk

**Russell Davis**  
*Partner, Banking and Capital Markets*  
+44 (0) 20 7007 6755  
rdavis@deloitte.co.uk

**Matt Cox**  
*Director, Insurance*  
+44 (0) 20 7303 2239  
macox@deloitte.co.uk

**Terri Fielding**  
*Partner, Investment Management and Private Equity*  
+44 (0) 20 7303 8403  
tfielding@deloitte.co.uk

**Mike Sobers**  
*Partner, Technology*  
+44 (0) 20 7007 0483  
msobers@deloitte.co.uk

**Kevin Doherty**  
*Partner, Scotland*  
+44 (0) 141 304 5711  
kedoherty@deloitte.co.uk

**Jamie Young**  
*Partner, Regions*  
+44 (0) 113 292 1256  
jayoung@deloitte.co.uk

## Risk and Regulation

**Tim Thompson**  
*Partner, Quantitative Risk and Finance*  
+44 (0) 20 7007 7241  
tthompson@deloitte.co.uk

**Stephen Boyd**  
*Senior Manager, Risk and Regulation*  
+44 (0) 141 314 5893  
sboyd@deloitte.co.uk

**Ally McGeorge**  
*Manager, Risk and Regulation*  
+44 (0) 131 535 7822  
amcgeorge@deloitte.co.uk

# Notes



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see [www.deloitte.co.uk/about](http://www.deloitte.co.uk/about) for a detailed description of the legal structure of DTTL and its member firms.

Deloitte LLP is the United Kingdom member firm of DTTL.

This publication has been written in general terms and therefore cannot be relied on to cover specific situations; application of the principles set out will depend upon the particular circumstances involved and we recommend that you obtain professional advice before acting or refraining from acting on any of the contents of this publication. Deloitte LLP would be pleased to advise readers on how to apply the principles set out in this publication to their specific circumstances. Deloitte LLP accepts no duty of care or liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

© 2014 Deloitte LLP. All rights reserved.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 2 New Street Square, London EC4A 3BZ, United Kingdom. Tel: +44 (0) 20 7936 3000 Fax: +44 (0) 20 7583 1198.

Designed and produced by The Creative Studio at Deloitte, London. 36845A