Deloitte.

Session 1 - How risk management can interact effectively with internal audit

Dominic Fisher, Deloitte Malta, 13 July 2016

How ‘Risk Management’ Can Interact Effectively With Internal Audit

Scene Setting For This Session

MFIA
Malta Forum for Internal Auditors

MARM
MALTA ASSOCIATION OF RISK MANAGEMENT

Forum – This session is intended to open a dialogue.

Risk Management – MARM is an association of risk management, not risk managers. Most organisations will have many individuals whose official role does not contain the word ‘risk’, but whose work is relevant to enterprise risk management efforts. In addition to recognised ‘risk managers’ this session is also aimed at you.

Contents

What Is Risk Management?

‘Risk management aims at creating a disciplined, structured and controlled environment within which risks to the organisation can be anticipated and maintained within predetermined acceptable limits’

Joint Guidance On Risk / Audit Committees

Risk & Internal Audit Co-ordination

Ideas At The Leading Edge

Audit and Risk Committees
News from EU Legislation and Best Practices

October 2014

Weblink
http://tinyurl.com/zox9y3s

The EU's 8th Company Law directive includes a requirement for Audit Committees at public interest organisations* to

'form an **independent** view on the effectiveness of **risk management** and **internal controls**'.

This is the backdrop for this piece of thought leadership.

*About 6,000 organisations across the EU

Key Points Arising

Define Committee roles and responsibilities by a Charter Terms of Reference

- The Guidance identifies 10 possible responsibilities to share between Audit and Risk committees – and how they could / should be allocated.
- Recommends the involvement of Heads of Risk / IA in Audit and Risk Committees.

Common Risk Management Approach

- This means a clearly communicated risk and control framework. For example, one would expect consistency in 'risk reporting' measurements between IA and Risk.
- If a common risk management approach is in place, you would expect Internal Audit to use Risk Management's outputs (e.g. risk register).

Reaffirms the 'Three Lines Of Defence' Model

- Board sets risk appetite and risk - taking philosophy.
- CEO and senior management responsible for managing of risks and internal control.
- Suggest enterprise risk mapping for second line of defence.
- Composition of second and third lines depends on resources, staffing and maturity of the organisation. Costs and benefits need to be balanced.

Following Up Internal Audit Work

Follow Up Internal Audit Work By Risk Management

Some Basic Expectations

Assisting line management with remediation efforts

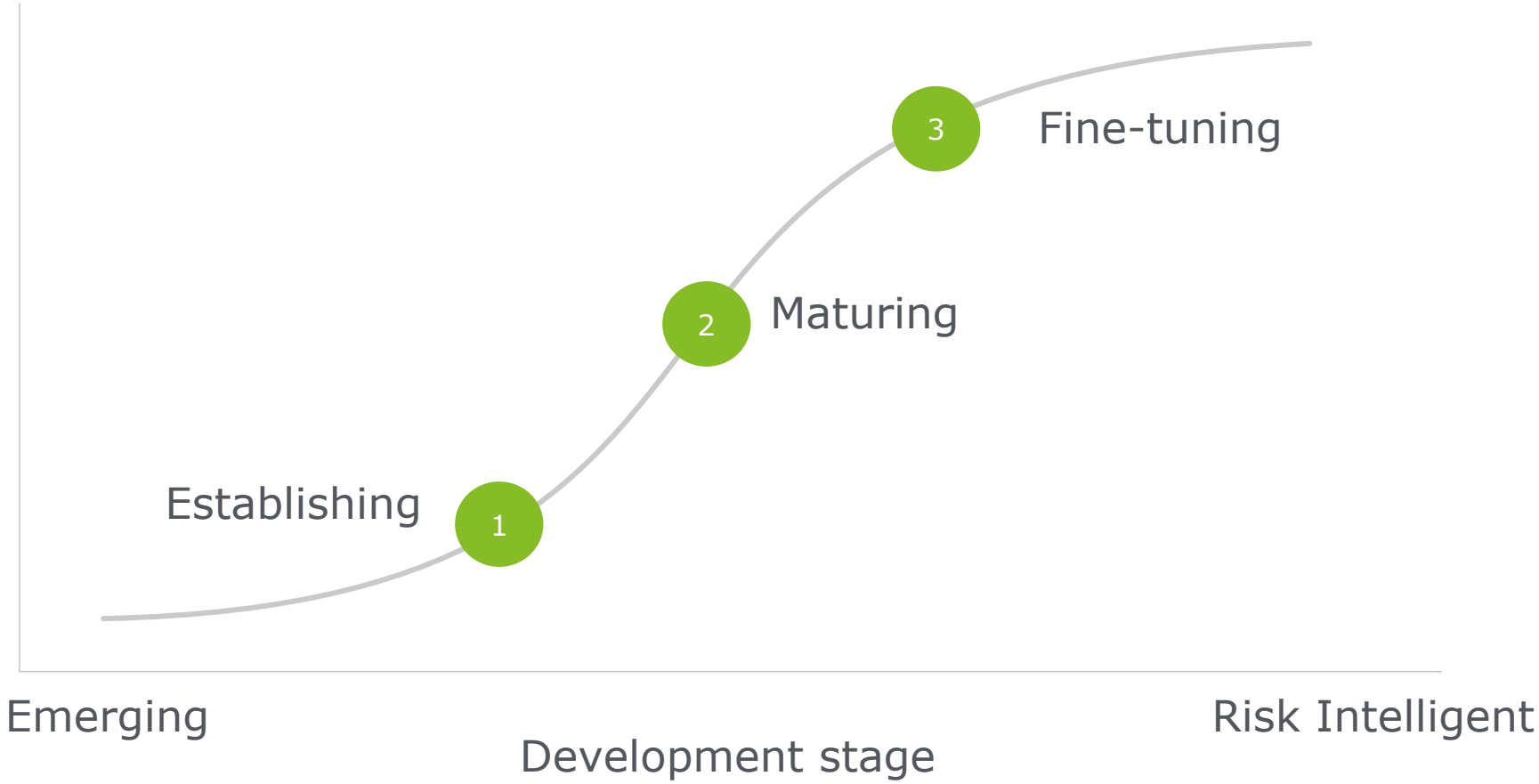
- Provide assistance with remediation, especially where line management don't have the resources and internal auditors are constrained by independence issues.
- Risk experts should be aware of and be able to advise on alternative risk treatments and also the risks arising from process change.
- Line managers should be aware of the availability of expert resource. Build a reputation which leads to line management requesting your input.

Using IA work as a feedback loop

- Internal audit findings with a bearing on risk should be shared with a suitable audience (e.g. Board of Directors, Risk Committee, Risk Steering Committee, Line Management etc).
- When relevant, internal audit results can be used to reassess the nature and quantum of relevant residual and inherent risks.

Synergistic Themes
Diagnosing Suitable Action

Risk Maturity Stages



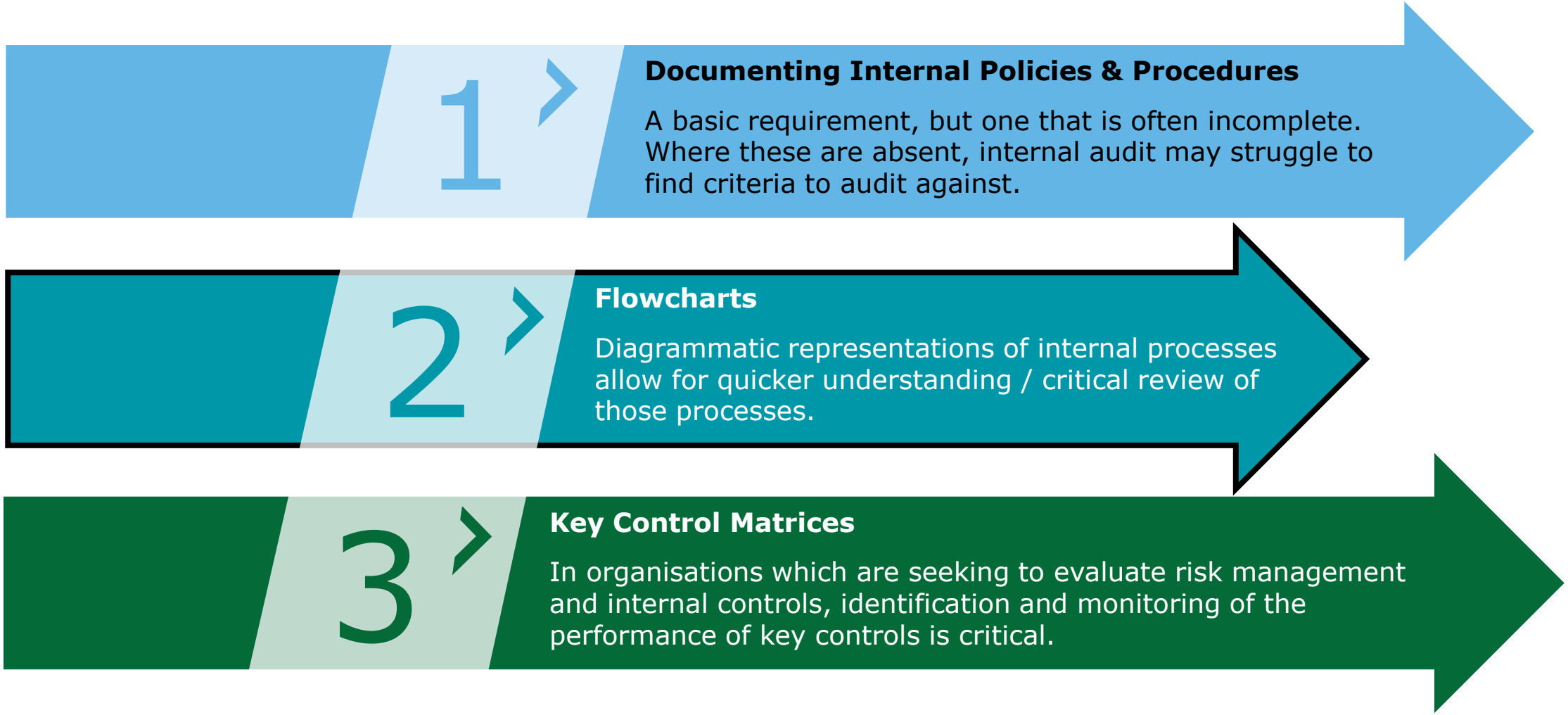
Suitable improvement recommendations depend on your organisation’s existing risk maturity.

Synergistic Themes

Formalising Policies & Procedures

Supporting Internal Audit

Formalising Policies & Procedures

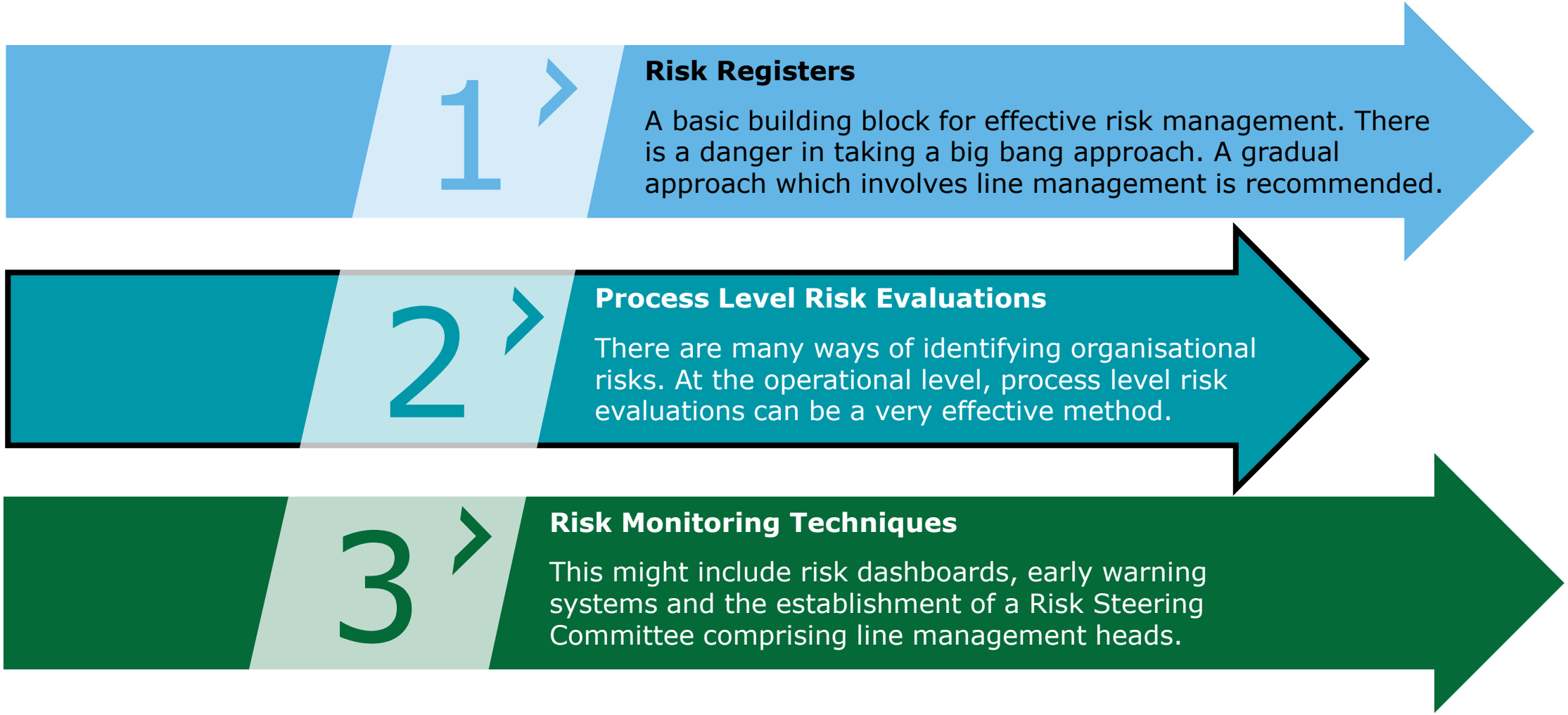


Synergistic Themes

Risk Evaluations

Supporting Internal Audit

Risk Evaluations



Supporting Internal Audit

Process Flowcharts & Process Level Risk Evaluations

Process Flowcharts

Diagrammatic representations of internal processes allow for quicker understanding / critical review of those processes.

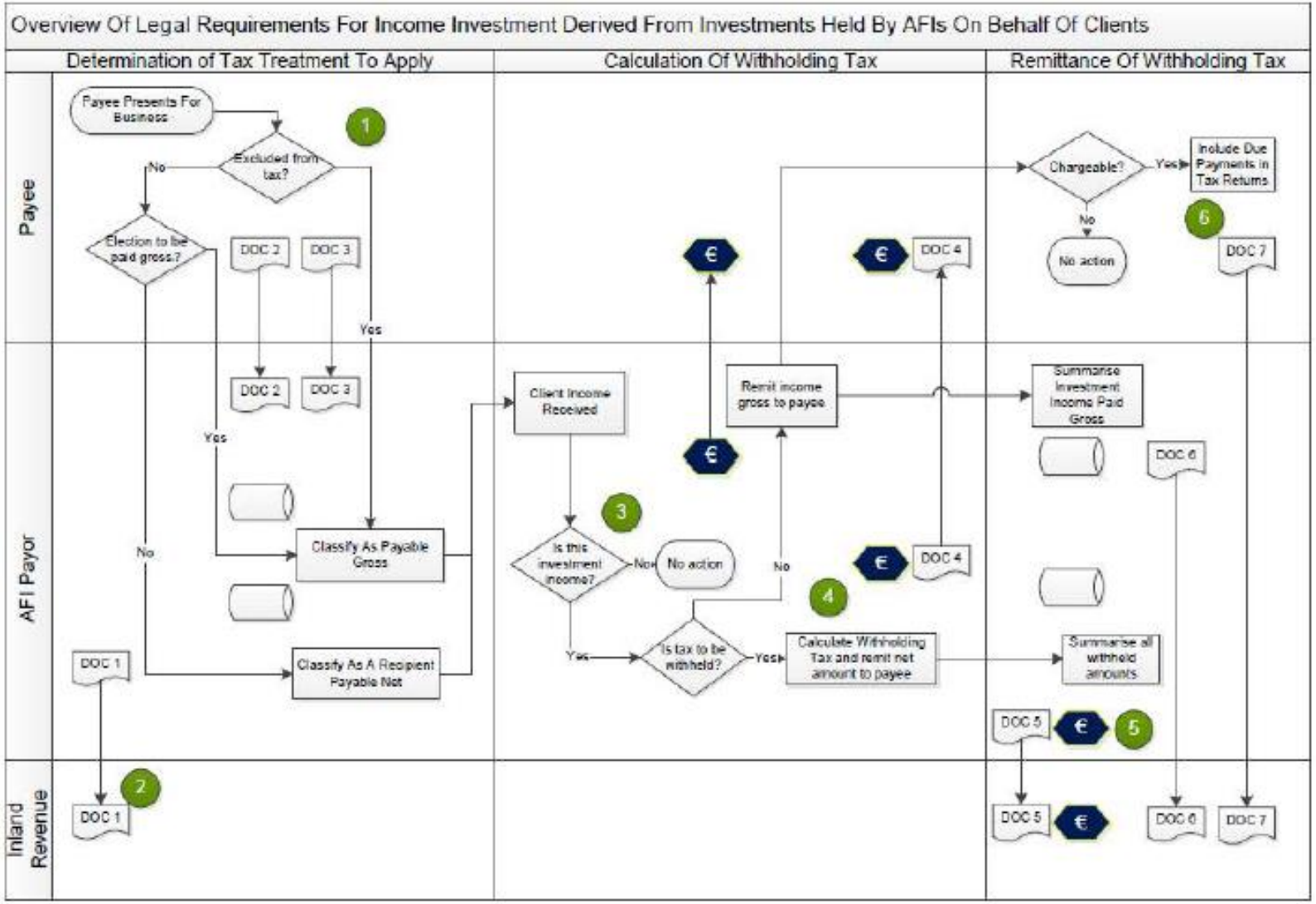
Process Level Risk Evaluations

There are many ways of identifying organisational risks. At the operational level, process level risk evaluations can be a very effective method.

A Written Overview of a Medium Complexity Process

An overview of legal requirements for income investment derived from investments held by authorised financial intermediaries (AFI) on behalf of clients follows. All AFI payors must register with the Inland Revenue. There is a risk that an AFI payor will not register with the Inland Revenue, but represent to clients that they are registered and then collect tax which is not remitted to the authorities. The process begins when a payee presents for business to the AFI payor. The payee must determine whether they are excluded from tax. There is a risk here that the payee will make an incorrect determination of their tax status. Nevertheless, if they do so, they are classified as requiring to be paid gross by the AFI payor as long as they can provide suitable evidence that they are excluded from tax in Malta. If not, the payee may still elect to be paid gross. In such circumstance they must notify the AFI payor in writing. If a payee is not excluded from tax and does not elect to be paid gross, they ought to be classified by the payor as a recipient payable net. AFI payors must maintain system records to classify all clients as either payable gross or net. When income is received on behalf of a client, the AFI payor must determine whether this is investment income. There is a risk that incorrect determinations are made at this stage. In the case, where the income is not determined to be investment income, there is no further action required of the AFI payor. However, if the income received is determined to be investment income, the AFI payor must next determine whether tax is to be withheld. There is a risk of error here. If no tax is determined to need to be withheld, income is remitted gross to the payee and the AFI payor ought to add this item to the list of investment income paid gross which is remitted to the Inland Revenue on an annual basis. Meanwhile the payee has to determine whether the income is chargeable at the end of the year and where that is the case include due payments within his annual tax return which is remitted to the tax authorities in the following reporting period. There is a risk that taxpayers will omit chargeable income. Where tax is to be withheld, the AFI payor must calculate the amount to be withheld. The net amount and a withholding tax certificate is passed to the payee. The withheld amounts are summarised by the AFI payor and should equal the amounts shown on issued certificates. This summary sheet should be sent to the Inland Revenue on a monthly basis. The withheld amounts are due to be sent by 30 September in the year following the year when the client income was received.

Flowcharts Are Better



Process Evaluation Points

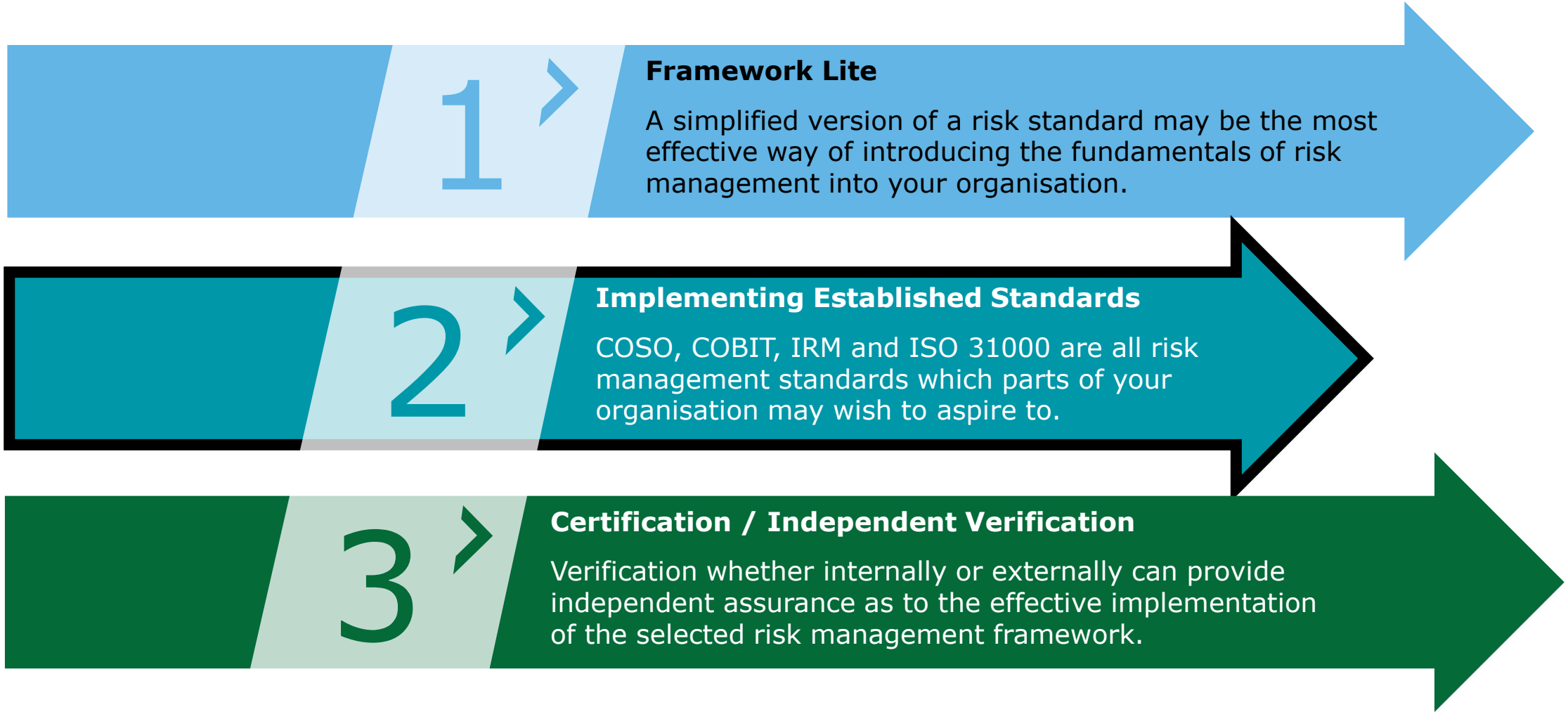
- A diagrammatic representation shows a chronological flow which is far easier to understand or explain.
- The involved parties and the nature of their involvement are clear.
- Decision Points, document flows, cash flows and system interfaces are clearly marked which provides a user with a clear appreciation of risk points and areas which may be ripe for improvement (e.g. automation, removal of duplicated processes)
- For each step (and across the entire process), users can consider classic audit risks (completeness, accuracy and validity) as well as efficiency.
- This type of document can assist efficient internal audit planning.

Synergistic Themes

Implementing Risk Management Frameworks

Supporting Internal Audit

Implementing Risk Management Frameworks



A Comparison Of Two Of The Most Common Risk Management Frameworks

COSO 2013 vs ISO 31000

COSO 2013

- Long
- US standard
- Focus on evaluations
- Emphasis on downsides
- Link to strategy
- Auditor’s view
- Can cherry-pick your focus (i.e. pilot test)

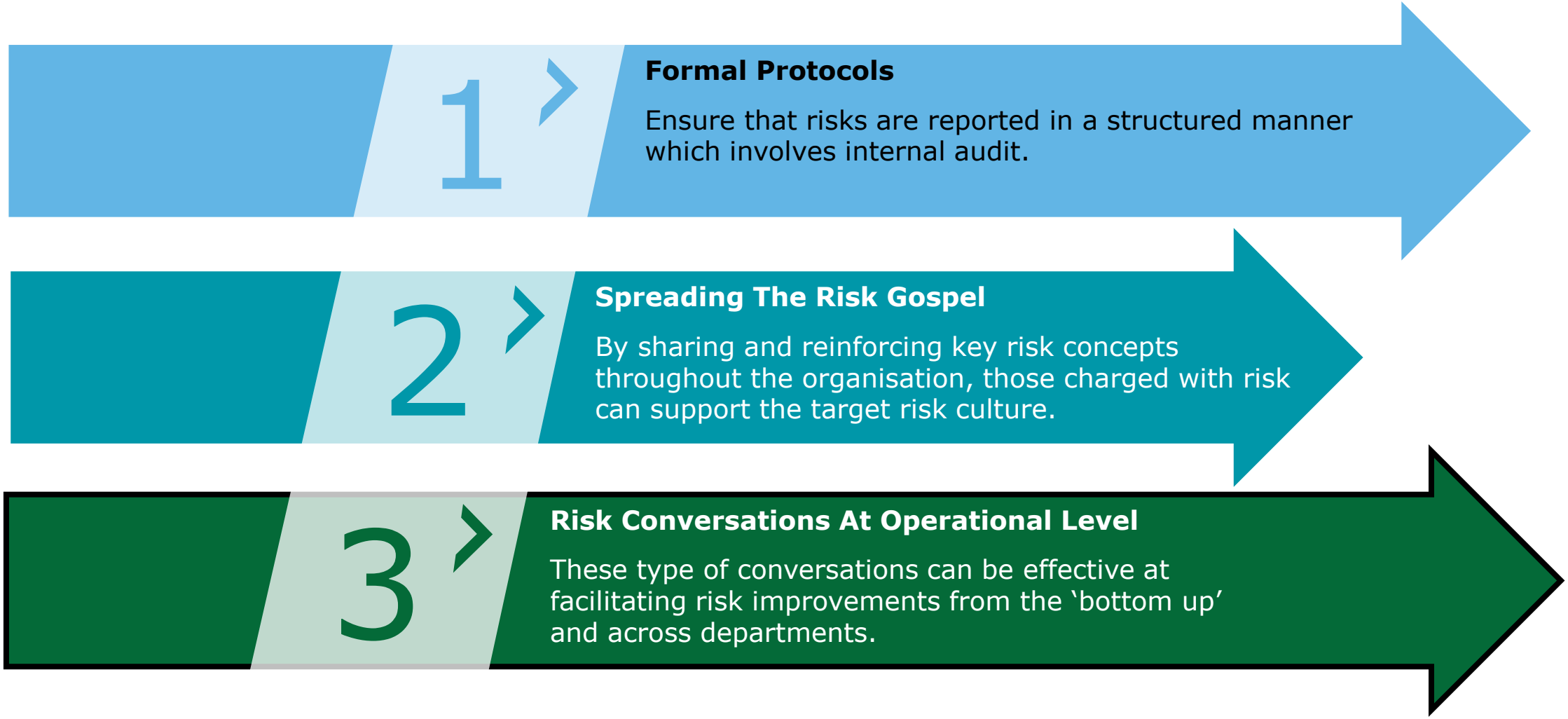
ISO 31000

- Short
- International
- Focus on enterprise risk management
- Neutral between risks and opportunities
- Little mention of risk appetite
- Risk manager’s view
- Provides a co-ordinated risk process

Synergistic Themes

Communication

Supporting Internal Audit
Communication



Healthy Conversations About Internal Controls

Achieving Improved Risk Management & Internal Control From The Bottom Up

To what extent did you carry out the controls which were prescribed or needed?

What were the problems in carrying out these controls?

Do you have any ideas to improve the efficiency and effectiveness of the controls for which you are responsible?

Based on your work how well do you think that processes and controls have worked in other areas?

How well do you think these controls have performed?

What do these findings suggest and what could we do better?

What findings did you have from performing your controls (errors, backlogs, missing information etc)

Wrapping Up

Concluding Comments

'It is important for organisations to set up an efficient and integrated corporate governance model'

Thijs Smit President of ECIIA

'When it comes to gaining synergies between risk and internal audit, build on what you have, taking into account your organisation's existing level of risk maturity'

Dominic Fisher, Deloitte Malta

'Audit and Risk Committees need to rely more than ever on competent risk and internal audit professionals.'

Julia Graham, President of FERMA

Deloitte.

Dominic Fisher

Senior Manager Enterprise Risk Services

dofisher@deloitte.com.mt