SOPAC®
LIVE THE EXPERIENCE
SOPAC 2015 Conference | Hilton Sydney Hotel
15 - 18 MARCH 2015

Benefits of Controls Frameworks – Putting COSO into Action

Anton van Wyk, CIA, QIAL, CRMA
IIA Global Chairman

Tania Stegemann, CIA, CCSA, FCA
Executive Audit Manager, Leighton Holdings

The Institute of Internal Auditors Australia

The Institute of Internal Auditors Australia

Contents

Using a Control Framework

IPPF Standard 2100 – Nature of Work

- The internal audit activity must evaluate and contribute to the improvement of governance, risk management and control processes, using *a systematic and disciplined approach*.

IPPF Standard 2200 – Planning

- Internal Auditors must develop and document a plan for each engagement….

IPPF Standard 2201 – Planning Considerations

- In planning the engagement, internal auditors must consider….
  - The objectives of the activity being reviewed and the means by which the activity controls its performance
  - The significant risks to the activity, its resources and operations and the means by which the potential impact of risk is kept to an acceptable level
  - The adequacy and effectiveness of the activity's risk management and control processes *compared to a relevant control framework or model*
  - The opportunity for making significant improvements to the activity's risk management and control processes

Framework Approach for evaluating controls

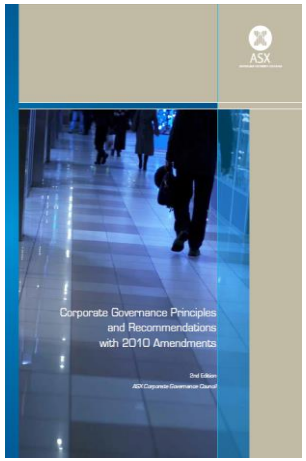
Management implements controls based on their perception of the risk exposures they face…

Controls may be designed to operate differently depending on the nature of the industry and organisation…

Auditors need some way to evaluate the many different management models and control processes they see – they need a framework

The Institute of Internal Auditors Australia

How does COSO fit into the governance model?



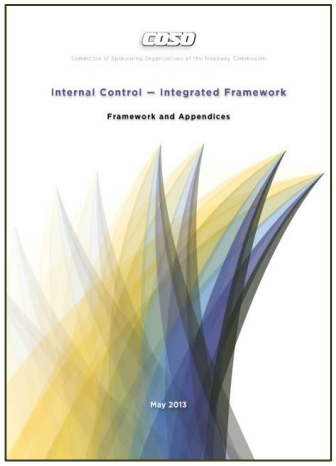
ASX Corporate Governance Principles and Recommendations

Eight principles, and supporting recommendations, including

- Principle 4: Safeguard integrity in financial reporting
- Principle 5: Make timely and balanced disclosure
- Principle 7: Recognise and manage risk

ISO 31000 – Risk Management Principles and Guidelines

- Principles
- Framework
- Process
  - Communication & consultation
  - Establishing the context
  - Risk assessment
  - Risk identification
  - Risk analysis
  - Risk evaluation
  - Risk treatment
  - Monitoring and review

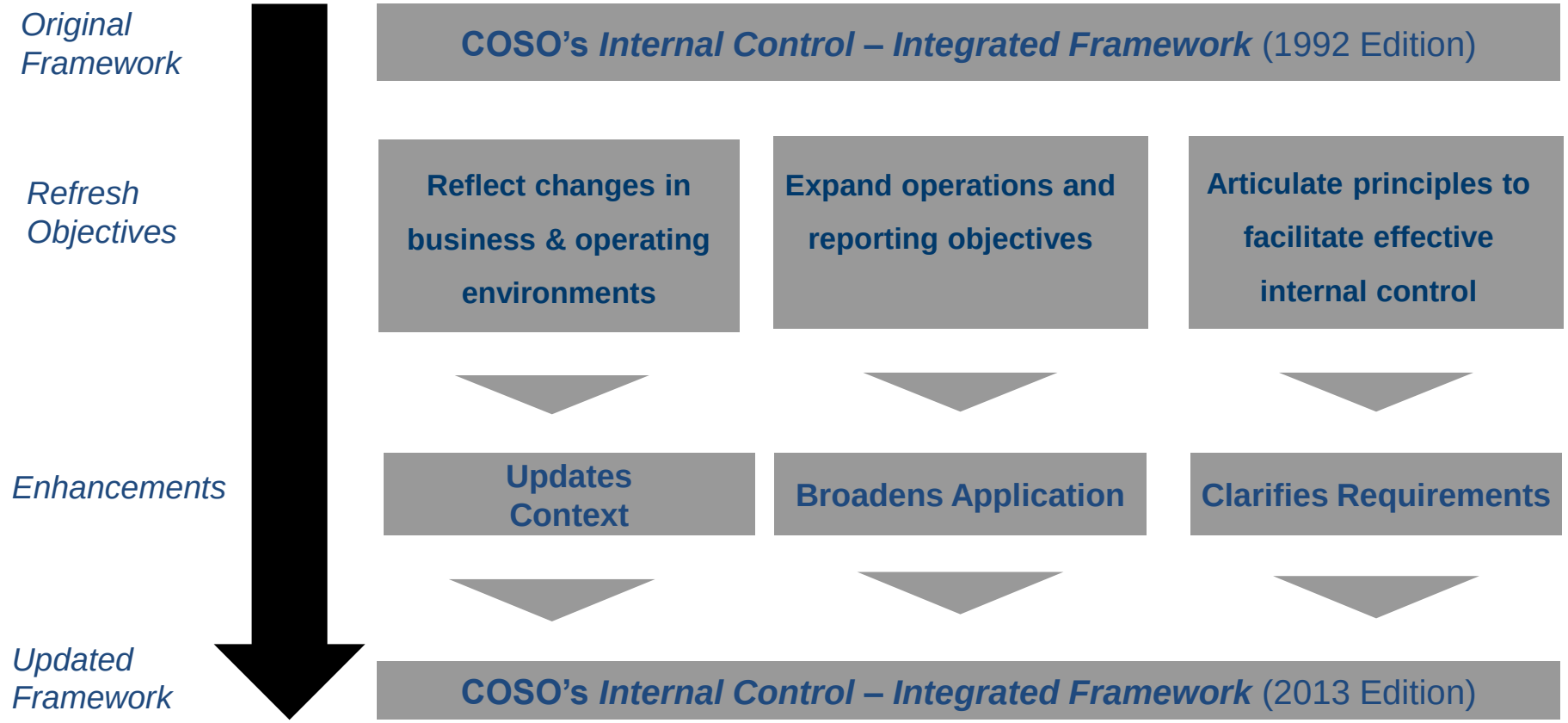


COSO Internal Control – Integrated Framework

- Five integrated components of internal control that support operations, reporting and compliance objectives, including:
- Control environment
- Risk Assessment
- Control Activities
- Information and communication
- Monitoring activities

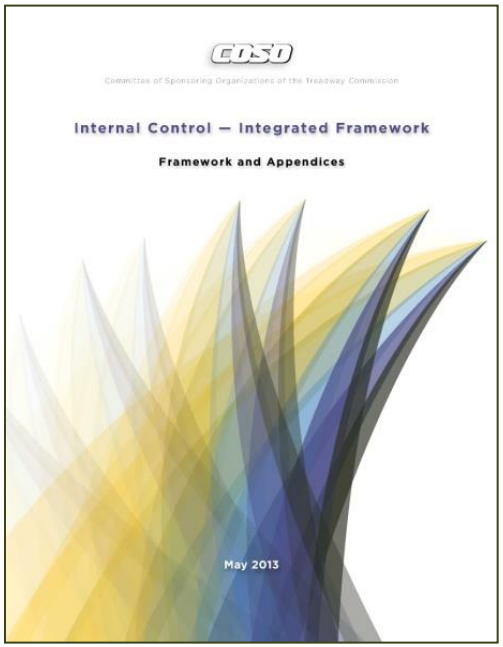
The Institute of Internal Auditors Australia

Evolution of the COSO Framework



COSO – Internal Control Integrated Framework

- Treadway Commission
- Standard Definition of Internal Control
- Achievement of objectives over three areas – Operations, Reporting and Compliance
- An effective control environment contains five elements
- Five elements further broken down into seventeen guiding principles



The COSO Internal Control – Integrated Framework

The definition of internal control

"Internal control is a process, effected by the entity's board of directors, management and other personnel designedd to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance"

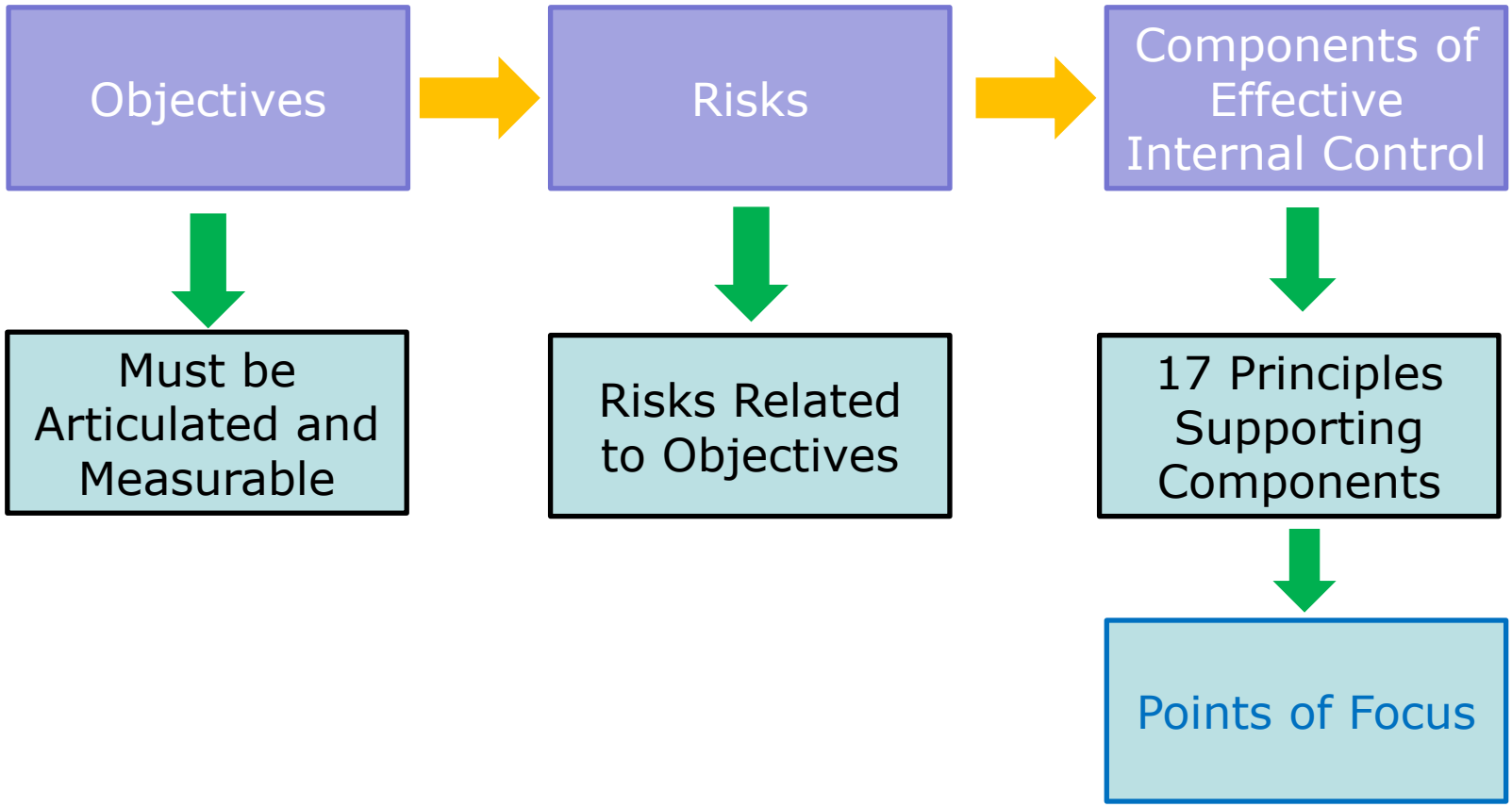
This definition reflects certain fundamental concepts

The Institute of Internal Auditors Australia

The COSO Internal Control – Integrated Framework

Control Environment	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
Risk Assessment	6. Specifies suitable objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change
Control Activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys through policies and procedures
Information & Communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring Activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

COSO – In summary



Operation of the Framework

- Internal Control needs to be integrated
- All five components need to work together to accomplish the relevant objectives
- When assessing controls, you need to ask
  1) is each component present and functioning?
  2) do the five components work together to provide “reasonable assurance” that relevant objectives will be met?
- A component is present and functioning when no major deficiencies have been identified in any of the principles related to the component – a deficiency in one principle cannot be compensated by strong operation of another principle
- Each of the five components need to be operating together – an aggregation of minor deficiencies across components may lead to a major deficiency being determined for the overall control assessment

The Updated Framework – focuses on trends and topics relevant to business today

Most businesses are planning changes that can impact controls

Major changes expected at organisations in the following areas over the next 12 months

Customer strategies	***31%***
Managing talent	***23%***
Organizational structure	***22%***
M&A, joint venture or strategic alliance	***22%***
Technology investment	***21%***

Source – PwC annual global CEO survey, Base of 1300 global CEOs.

Factors that have driven the need for a revised Framework and COSO's response

Heightened expectations for governance oversight and increased demands and complexities in laws, rules, regulations and standards	Accounts for a growing web of global regulations, e.g. financial reporting requirements and environmental standards
Globalisation of markets and operations	Explicitly considers business models and legal structures and helps apply controls in changing operating models
Greater complexity in your operating model and structure	Helps customise controls to ensure they are supporting multiple objectives and principles
Expectations for competencies and accountabilities	Greater emphasis on ensuring competent personnel are hired and are held accountable to the organisation, shareholders and the community
Expanding reliance on technology	Provides a principle directed at controls over technology - infrastructure, development, use, and links with other processes
Expectations relating to preventing/detecting fraud	Provides a principle directed at fraud risk assessment
New and evolving expectations for non- financial reporting	Extends to non-financial reporting objectives, e.g. sustainability reports and customer satisfaction measures

Increased focus on IT Risk

Directors want their organisation' s strategy and IT risk mitigation better supported through improved IT understanding at the board level

The "IT confidence gap"

- Most directors are between 60 and 70 —majority of professional lives in pre-digital era
  - Rapid pace of technological change
- Less than 1% of directors have been or are currently CIOs
  - IT can be a complicated and intimidating subject
- Highly technical jargon
  - Directors want more information to better understand IT
- Board time is at a premium: majority of directors spend only 5% of their board hours on IT
  - Lack of IT guidance for boards
- 60% of boards want to spend more time on IT

Application of the COSO internal control framework

Beneficial for all **"three lines of defense"**

- Business management
- Risk Management
- Internal Audit

Illustrative examples …

- Process and cost improvement
- Risk profiling and use of key risk and control indicators
- Audit findings and recommendations
- Root cause analysis
- Assessment of control environment

Business Management and Process Improvement

See the big picture

Specify objectives that matter to your business and would benefit from applying a comprehensive, integrated control system -

- Which recent strategic, business, or operating decisions have introduced new risks?
- How do our controls adapt to change? Is our organisation prepared to respond to change?
- Do we apply controls to objectives relating to internal reporting, non-financial reporting, operations, and compliance?
- Have we considered the entire organisation?

Lessons from the past

- What breakdowns have we experienced with our existing controls? Why didn't we anticipate them?
- What issues could have been prevented if we had greater internal control at the root cause?
- How can we strengthen our systems of internal control by better connecting objectives, risks, and controls?

Map relevant principles to existing controls

- How thoroughly have we implemented the fundamental concepts set out in the 1992 framework?
- Have we overlooked any principles in the design of our controls?

Business Management and Process Improvement cont.

Preparing your People

- helps you address people at all levels of the organisation, includes a principle for attracting, developing, and retaining competent personnel

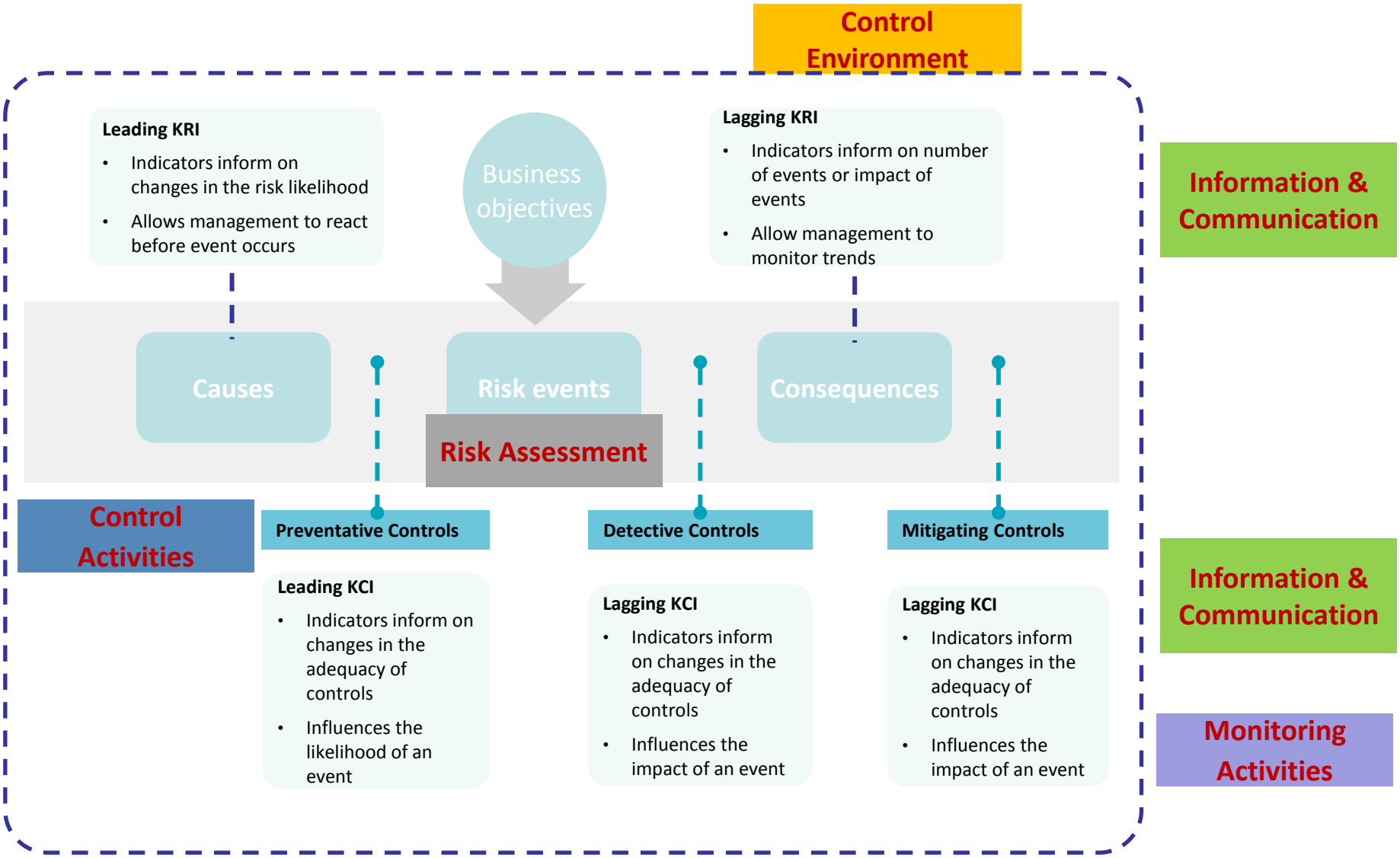
Understanding technology risks

- Overreliance on technology can introduce risks and mask problems
- Especially true for mobile, social, cloud, and other emerging technologies
- Update includes a principle explicitly focused on controls over the use of technology

Zeroing in on the right information and processes

- Includes several principles for using relevant information and communicating the right information to the right people
- Also addresses your significant processes and reminds businesses that they cannot delegate responsibility for achieving key objectives to business partners or service providers

Risk Management



Internal Audit – overall considerations

- Appoint a leader to marshal the transition to the updated framework
  - what is our board's view on broadening use of internal control and implementing the COSO Update?
  - how can we use the COSO Update to re-engage executives and the board in strengthening our systems of internal control?
  - how do we engage divisions, operating units, operations, internal audit, risk management, compliance, finance, technology, and human resources in adopting the updated framework?
- Assess whether your controls are really keeping up given the pace of change
- As business evolves, leading companies evolve their internal control systems – use the updated framework to consider whether the key risks have been identified and controls are present and functioning

Internal Audit – use of COSO in individual audits

- Ensure that the COSO elements are understood by the audit team and are considered during the development of the scope document and audit work program
- Provide guidance for specific COSO elements that are applicable to your organisation
- Provide training and education for management and staff on the elements and principles required for a fully effective control environment

Internal Audit – use of COSO to frame audit recommendations

Criteria

- What SHOULD be in place

Condition noted

- What IS actually in place (number of exceptions/dollar amount of exceptions out of total population value etc)

Root Cause

- Root cause of Condition

Consequence

- The impact / risk exposure of the Condition if left untreated

Proposed recommendation

- Possible recommendation. The Closing Meeting should be used as a Solutions Workshop to agree the management action.

COSO can be used to frame the criteria

COSO can be used to classify the root cause

COSO can be used to consider the aggregate findings

Conclusion

Achieving alignment of objectives and critical risks is a significant step towards internal audit improving its credibility, relevance and value to the business

Connect with the audit committee, confirm traditional coverage over financial and non-financial controls, IT, fraud and ethics – propose increased coverage in less traditional areas

Show competence in being able to tell the story and not just write it – help solve problems through objective eyes

Communicate the value you bring through the recommendations you provide and your involvement in emerging issues, rather than classic measures such as successful completion of the audit plan

CAEs need to show courage, leveraging strategic plans across the organisation in order to stay the course of alignment on expectations whilst delivering value

The Institute of Internal Auditors Australia

Questions