



The Institute of  
Internal Auditors  
Indonesia

# 2014 ACIIA CONFERENCE BALI, INDONESIA

**ASIAN CONFEDERATION OF INSTITUTE OF INTERNAL AUDITORS**

**The Stones Hotel - Legian, Bali**

**24 - 25 November 2014**

Organized by:



Supported by:



# **Integrating Organisational Objectives, Risks, Controls and Internal Audit Processes**

**Phil Leifermann**

**Acting Chairman, IIA Indonesia**

**Managing Director, Insight Consulting**



# Agenda

- **Introduction**
- **Objectives**
- **Risks**
- **Controls**
- **Assurance**
- **Risk Management**
- **Internal Audit**
- **Conclusion**

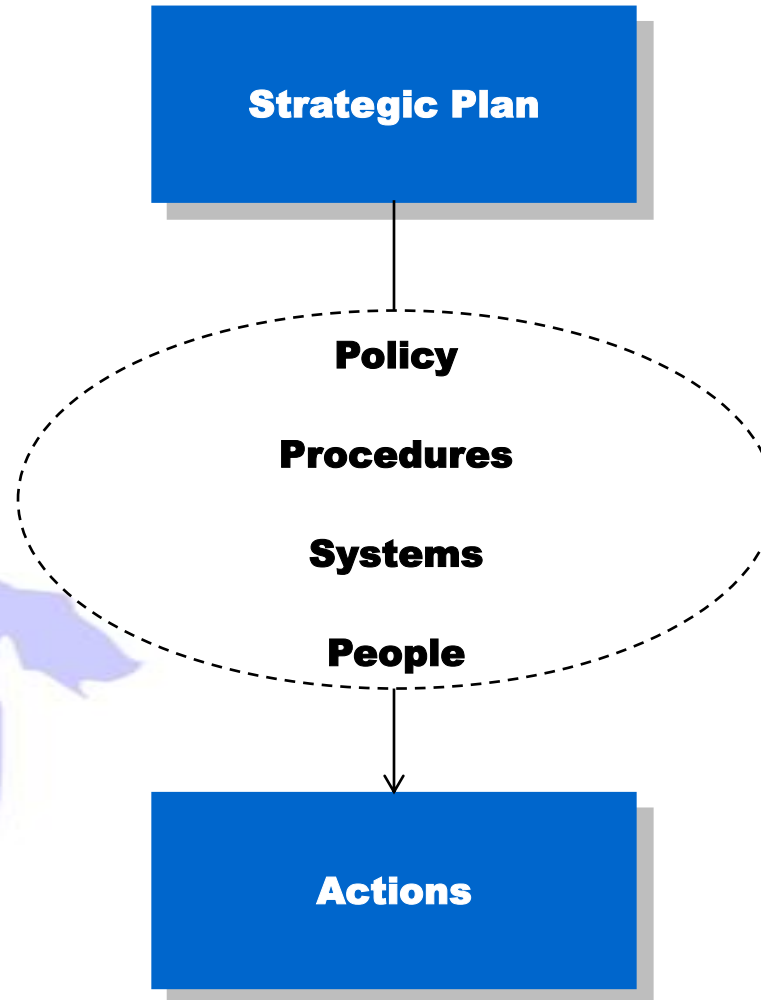


# **Agenda (cont.)**

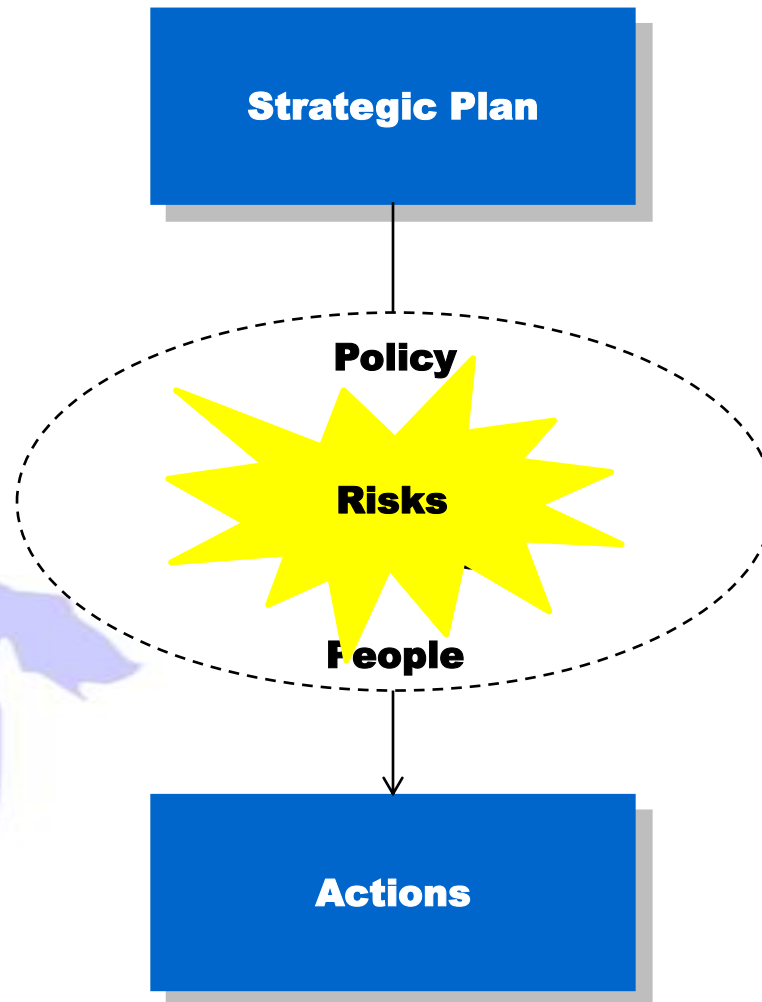
# **Back to basics !**



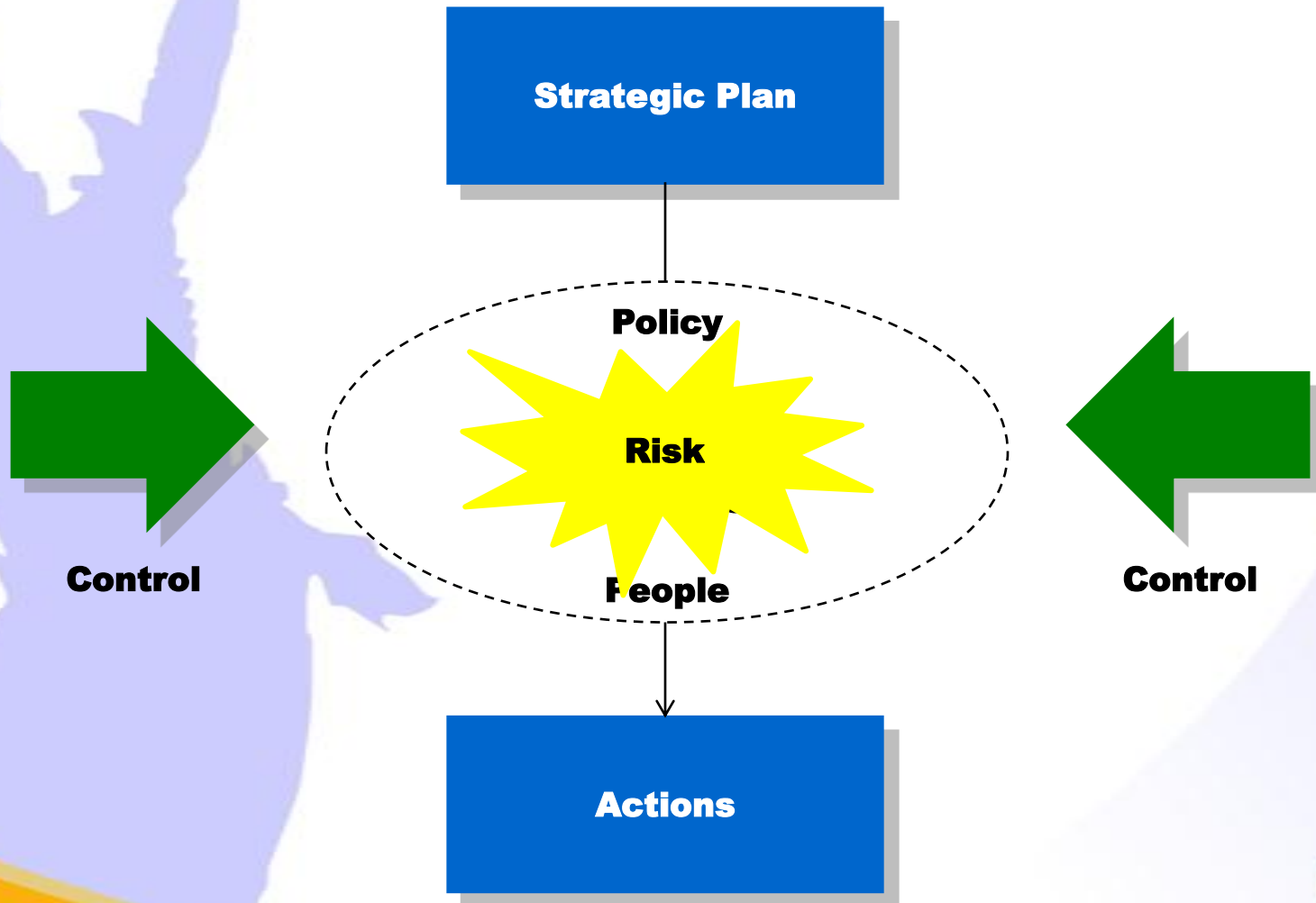
# Introduction



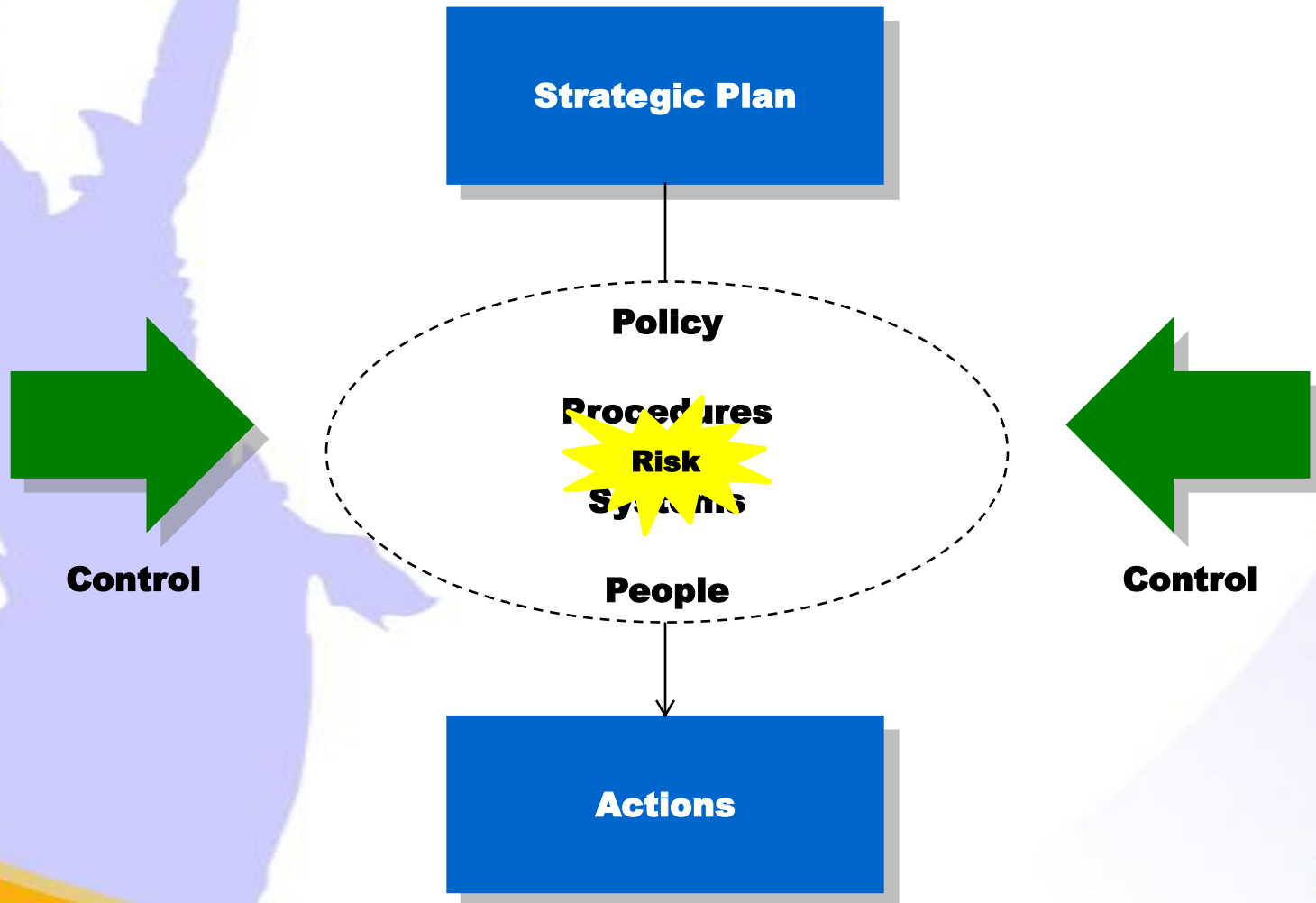
# Introduction (cont.)



# Introduction (cont.)

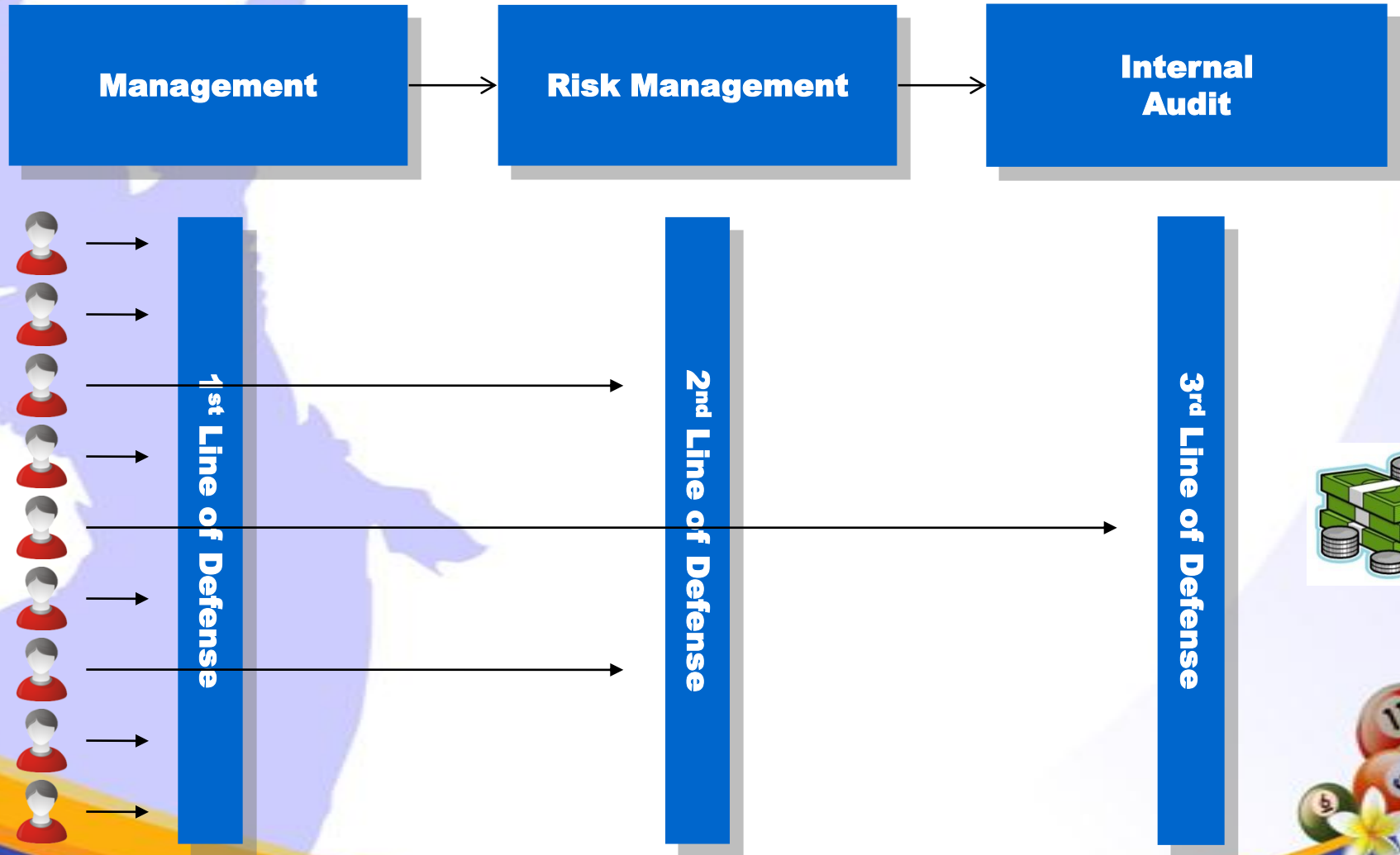


# Introduction (cont.)





# Introduction (cont.)



# Introduction (cont.)



- **Management are responsible for risks and controls**
- **Risk management are responsible for assisting management with risks and controls**
- **Internal audit are responsible for independently assessing risks and controls**



# Objectives

- **Anyone involved in management of risks must understand business**
- **In addition, they must understand strategic plan, as well as related goals and objectives**

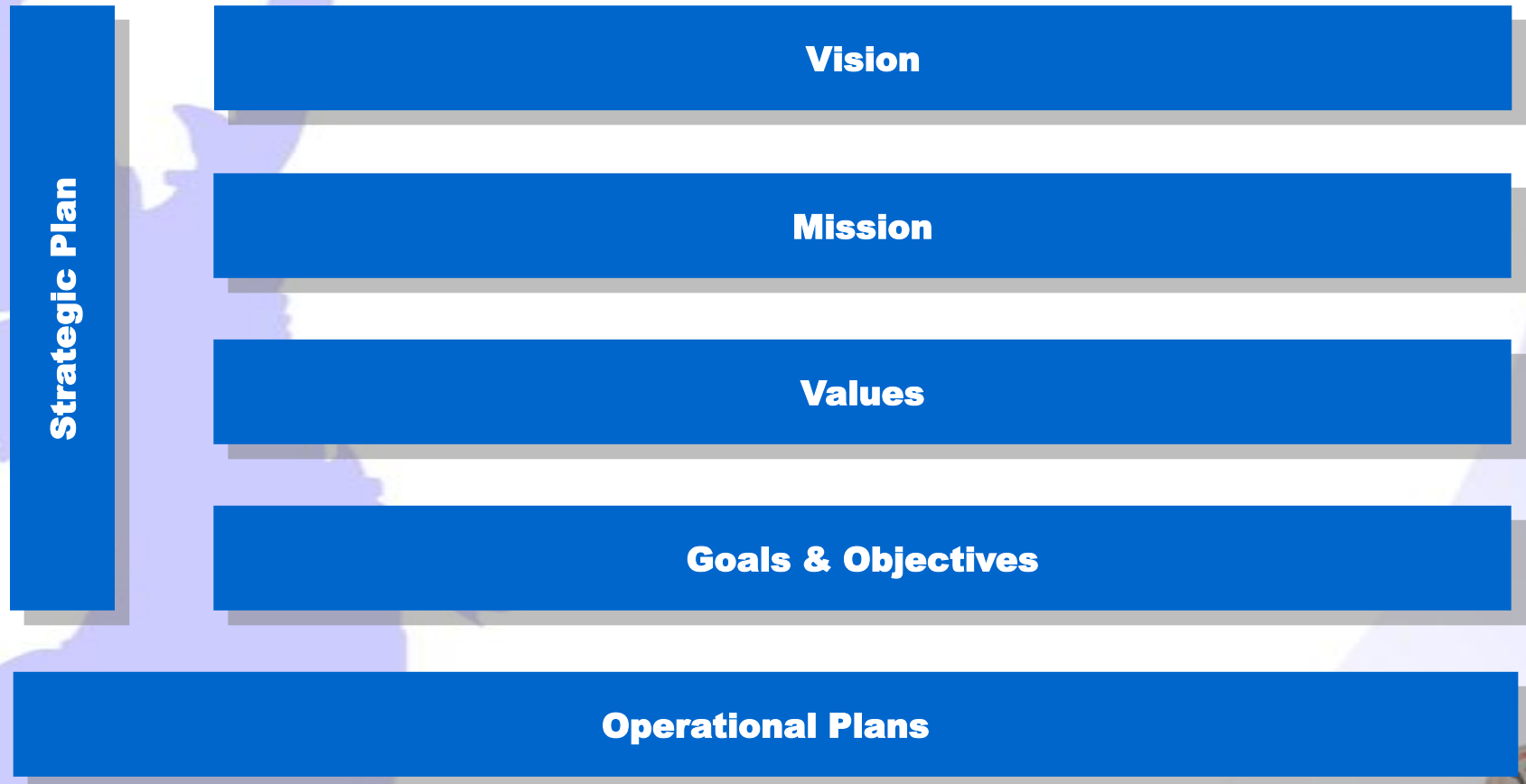


## **Objectives (cont.)**

**“If you fail to plan, you plan to fail”**



# Objectives (cont.)



# Objectives (cont.)

## Vision

- **Short, inspirational statement which expresses future of organisation**

## Mission

- **Short statement which describes organisation's "reason for being", including "what ?", "who ?", "how ?" and "why ?"**



# Objectives (cont.)

## Values

- **Underlying principles which govern behaviour of organisation and its people**

## Goals

- **Things we must do to be successful**



# Objectives (cont.)

## Objectives

- **Specific outcomes which must be achieved to satisfy these goals, including strategic, operational, financial and compliance**

## Operational plans

- **Shorter term action plans to achieve these goals and objectives**





# Objectives (cont.)



- **Where we are today**
- **Where we want to be in future**
- **Strategic plan shows what things we need to do to get from current status to desired status**
- **Operational plan shows how we do these things to get from current status to desired status**



# Objectives (cont.)

- **S Specific**
- **M Measurable**
- **A Actionable**
- **R Realistic**
- **T Timely**

abc

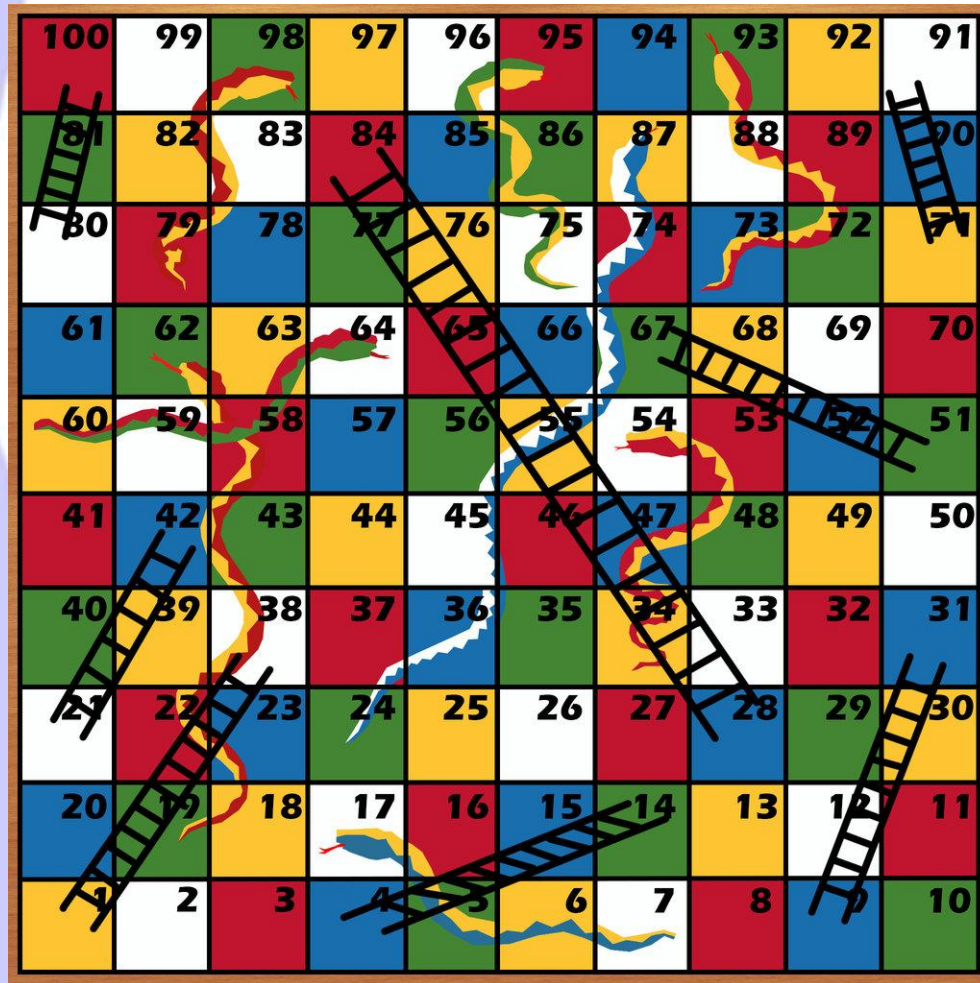


# Risks

- **Things that might occur which will effect organisation's objectives, whether positively or negatively**
- **These things which positively effect these objectives are usually known as opportunities**
- **These things which negatively effect these objectives are still known as risks**



# Risks (cont.)



A 10x10 grid with numbers 1-100. The grid is overlaid with a colorful illustration of a dragon. The dragon's body is composed of various colored segments: red, yellow, green, blue, and white. The dragon's head is red, and its tail is yellow. The dragon is positioned diagonally across the grid, from the bottom-left towards the top-right. Several black ladders are placed on the grid, some overlapping the dragon's body. The ladders are positioned at various points: one at the top-left, one at the top-right, one in the middle-left, one in the middle-right, one at the bottom-left, and one at the bottom-right. The grid is numbered from 1 to 100 in a standard font, with the numbers 1-10 in the bottom row, 11-20 in the second row from the bottom, and so on, up to 100 in the top-left corner.

100	99	98	97	96	95	94	93	92	91
81	82	83	84	85	86	87	88	89	90
80	79	78	77	76	75	74	73	72	71
61	62	63	64	65	66	67	68	69	70
60	59	58	57	56	55	54	53	52	51
41	42	43	44	45	46	47	48	49	50
40	39	38	37	36	35	34	33	32	31
21	22	23	24	25	26	27	28	29	30
20	19	18	17	16	15	14	13	12	11
1	2	3	4	5	6	7	8	9	10



# Risks (cont.)



- **Risks aren't isolated events**
- **Trigger, intermediate and risk event**
- **Consequence and impact**



# Controls

- **Things to be done to mitigate risks**

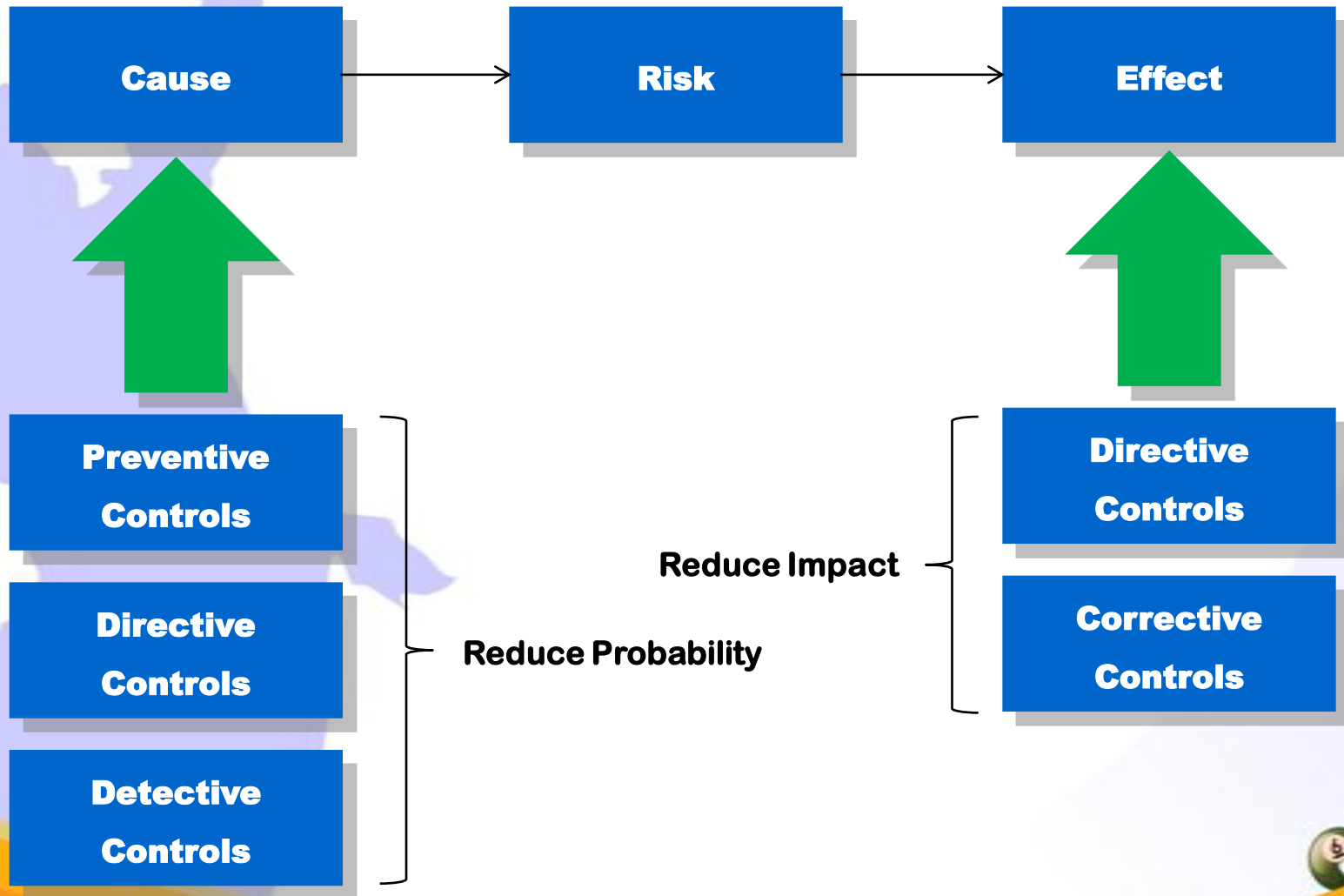


# Controls (cont.)

- **Preventive controls**
- **Directive controls**
- **Detective controls**
- **Corrective controls**

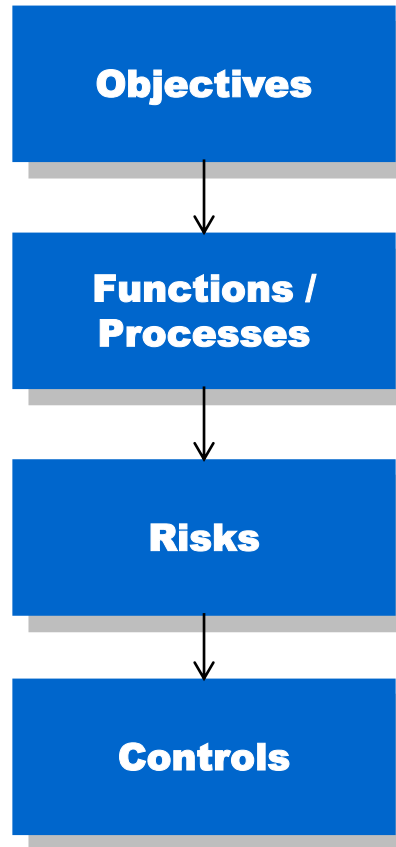


# Controls (cont.)





# Let's recap . . . . .

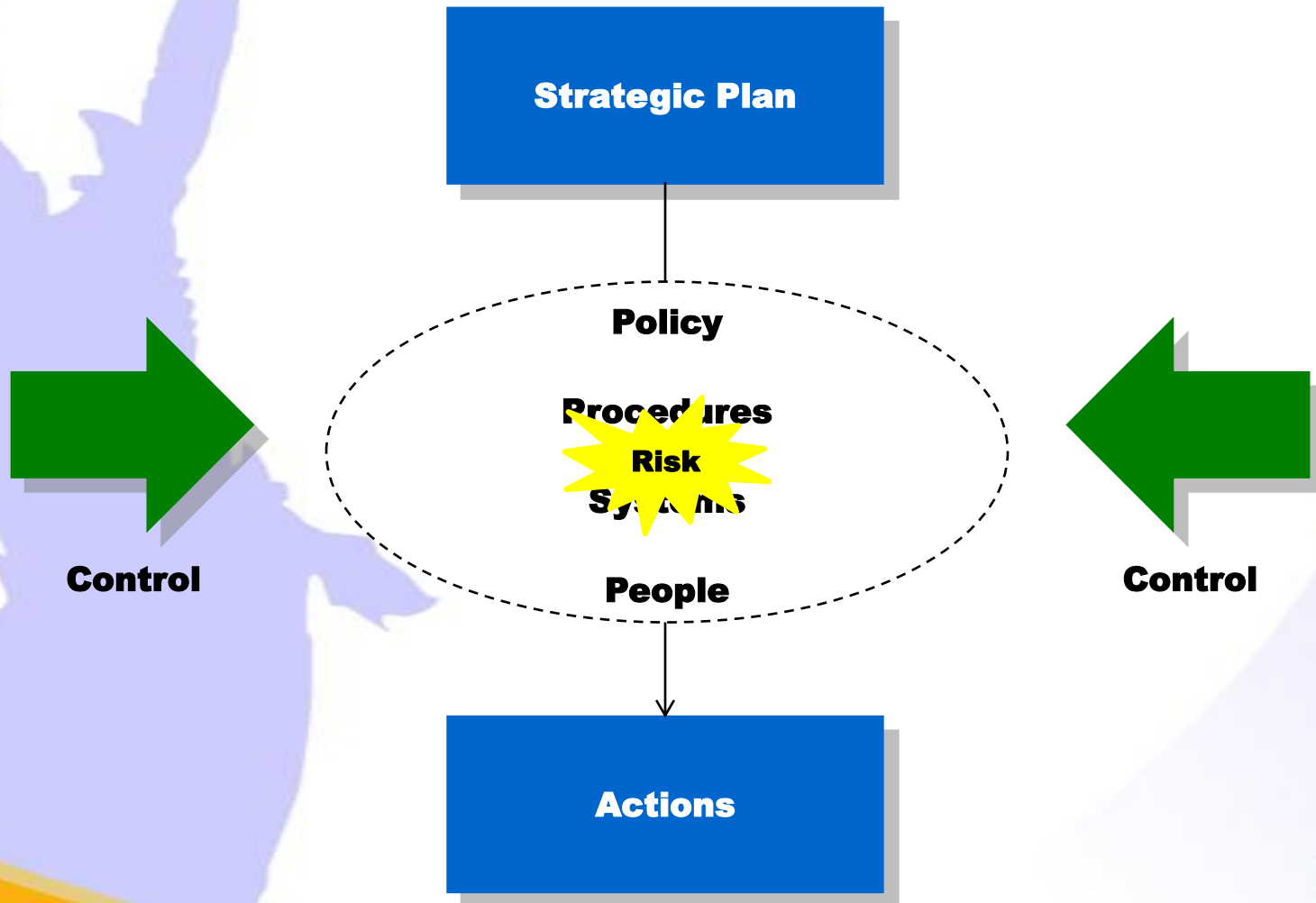


# Assurance

- **Process of evaluating organisation's management of risks and controls**



# Assurance (cont.)



# Assurance (cont.)

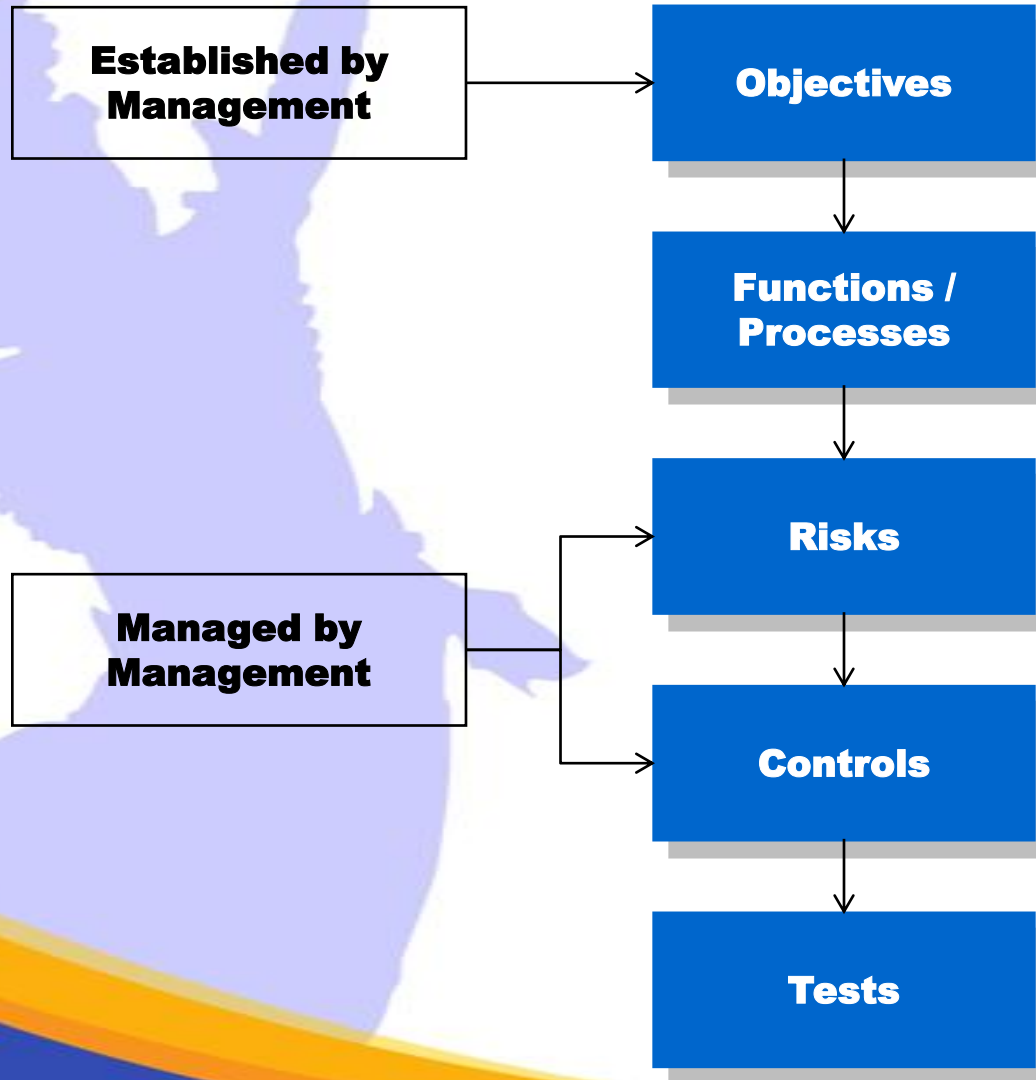


# Assurance (cont.)

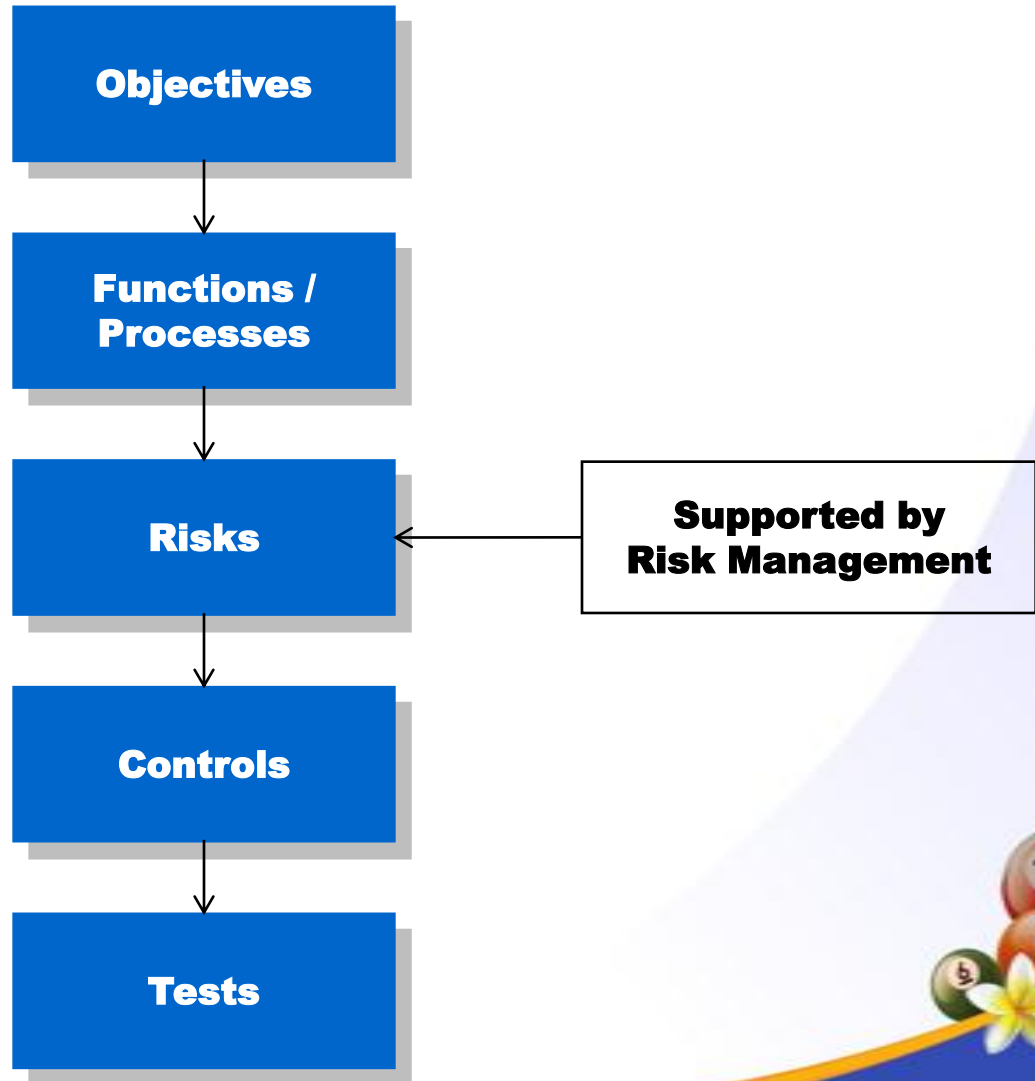
- **Risk management**
- **Compliance**
- **Internal audit**



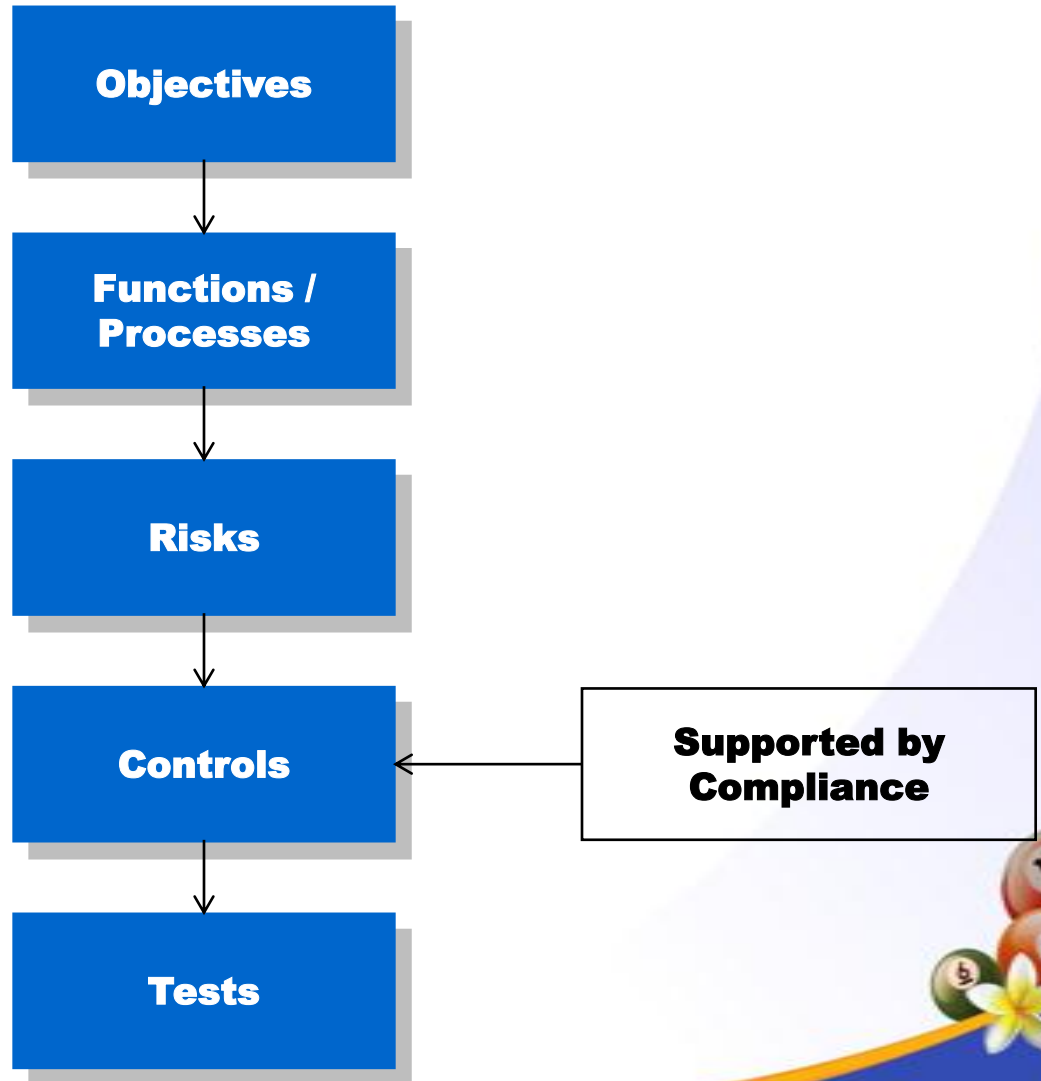
# Assurance (cont.)



# Assurance (cont.)

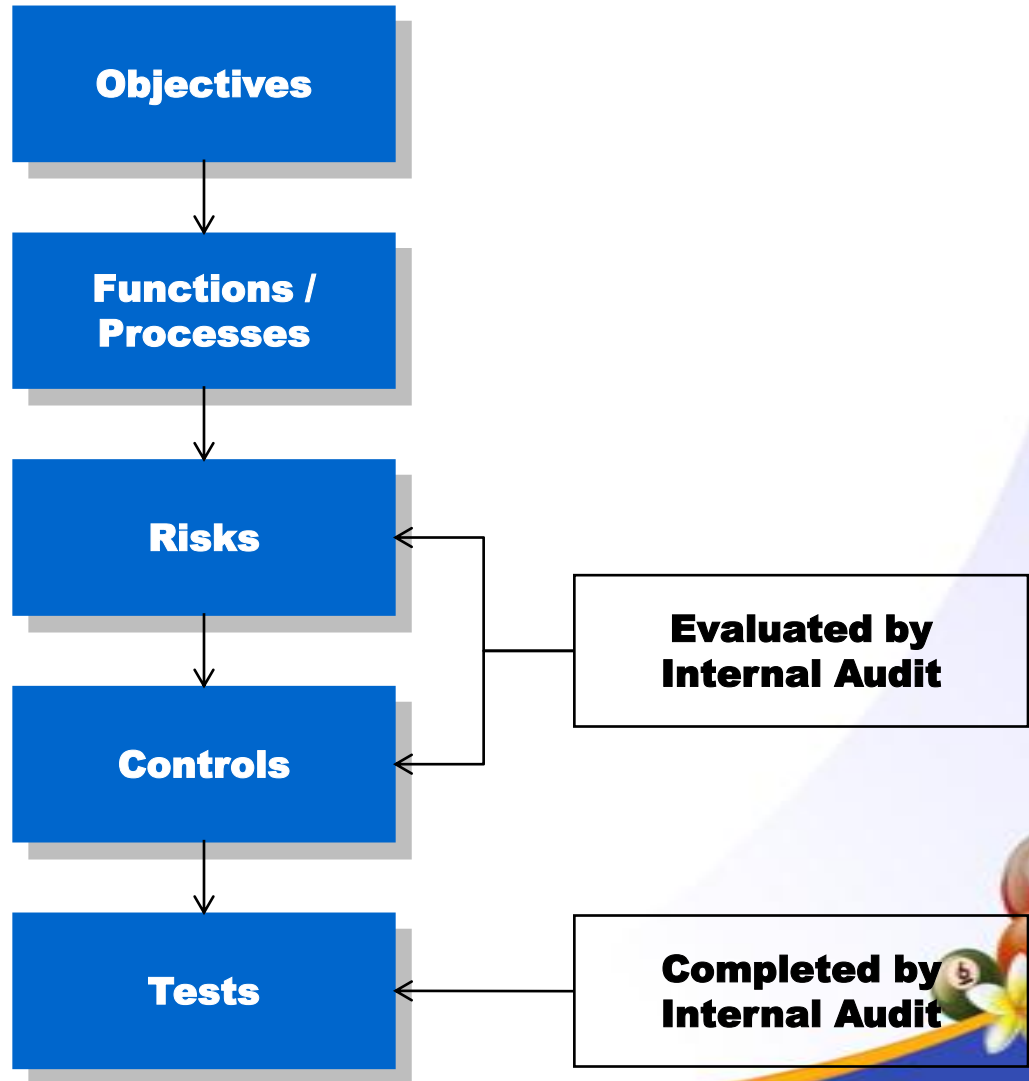


# Assurance (cont.)

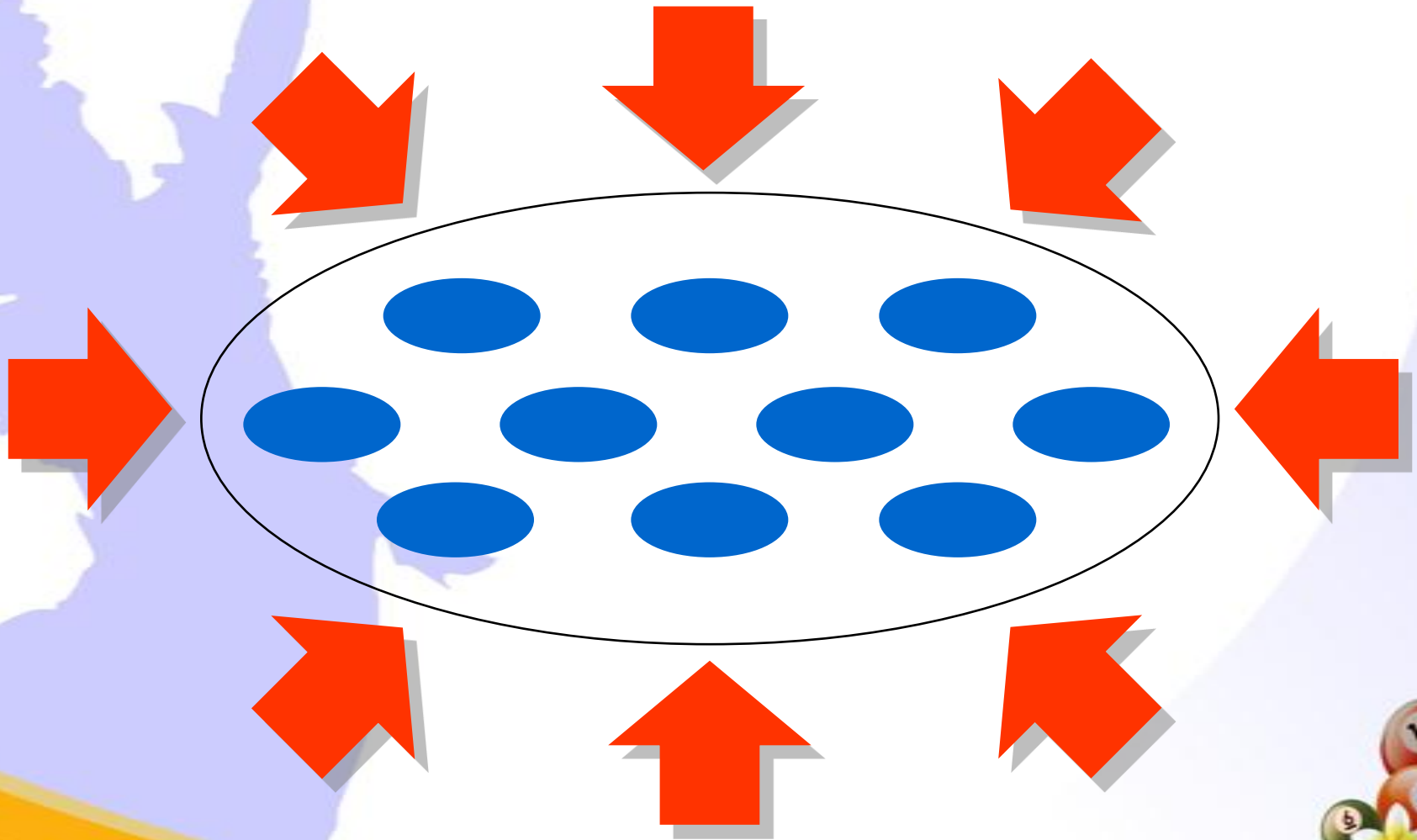




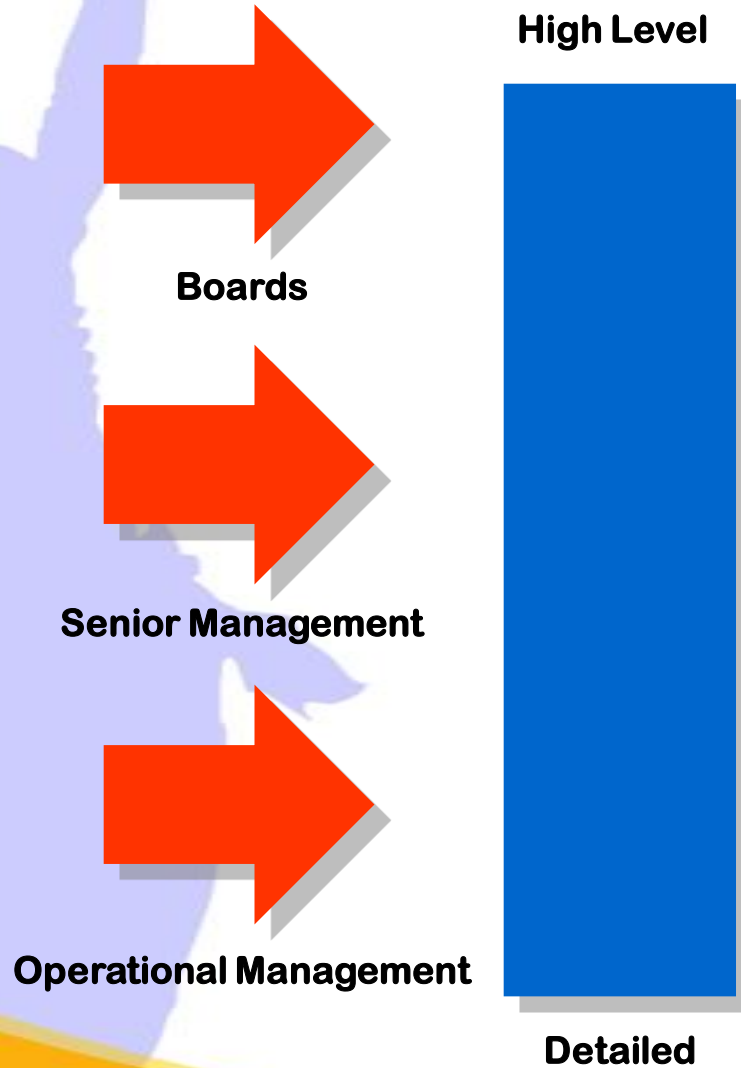
# Assurance (cont.)



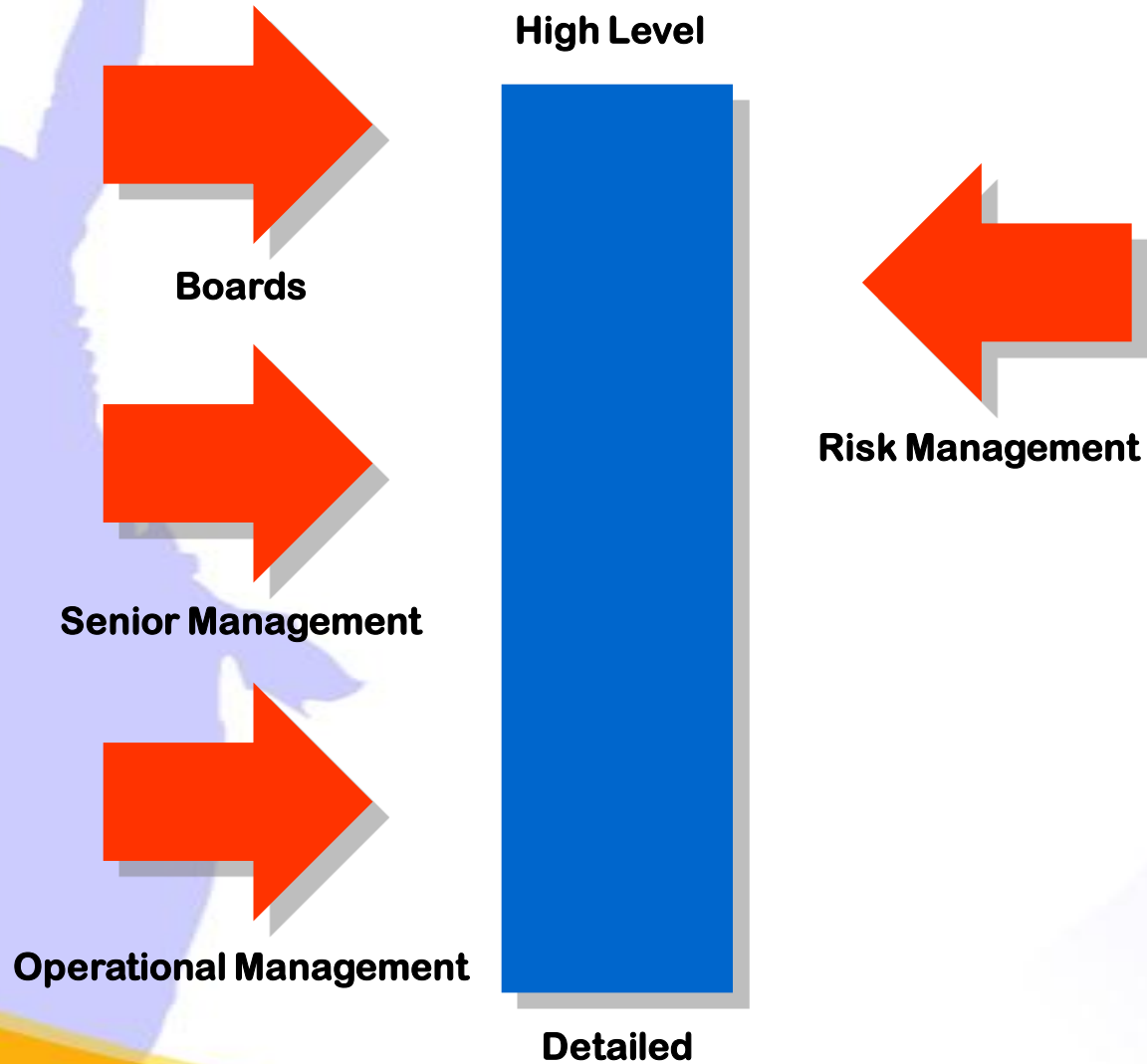
# Assurance (cont.)



# Assurance (cont.)

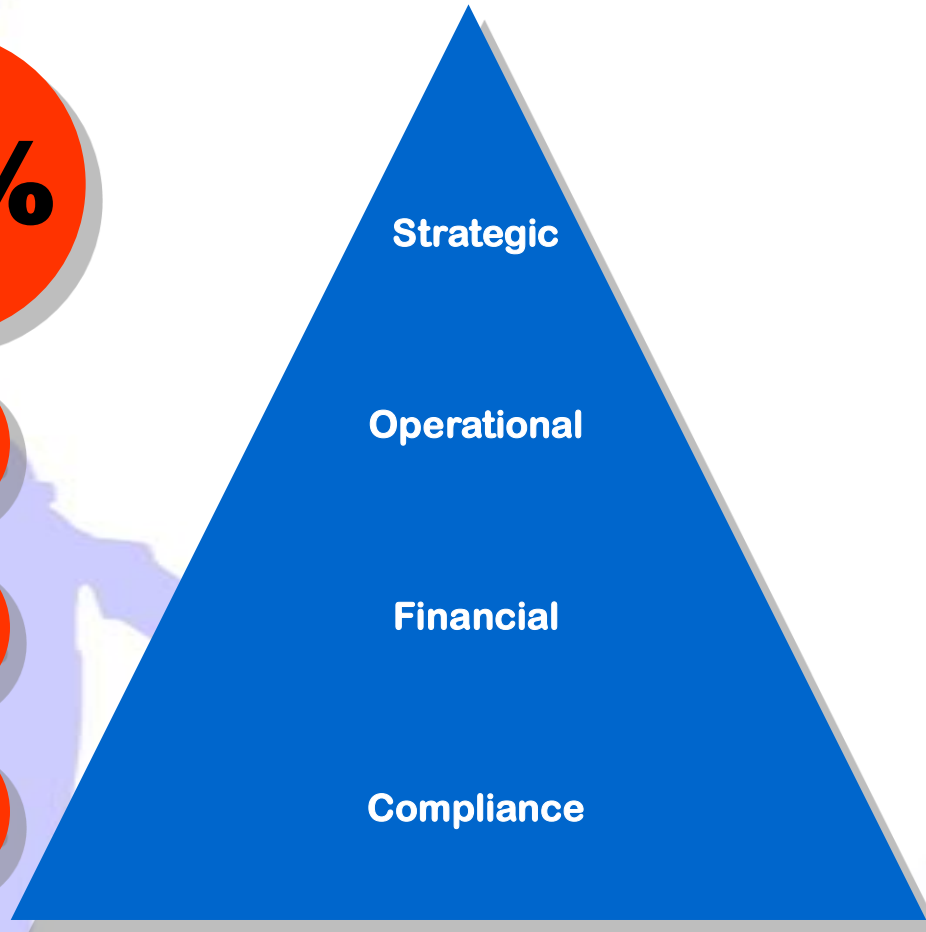


# Assurance (cont.)



# Assurance (cont.)

Management

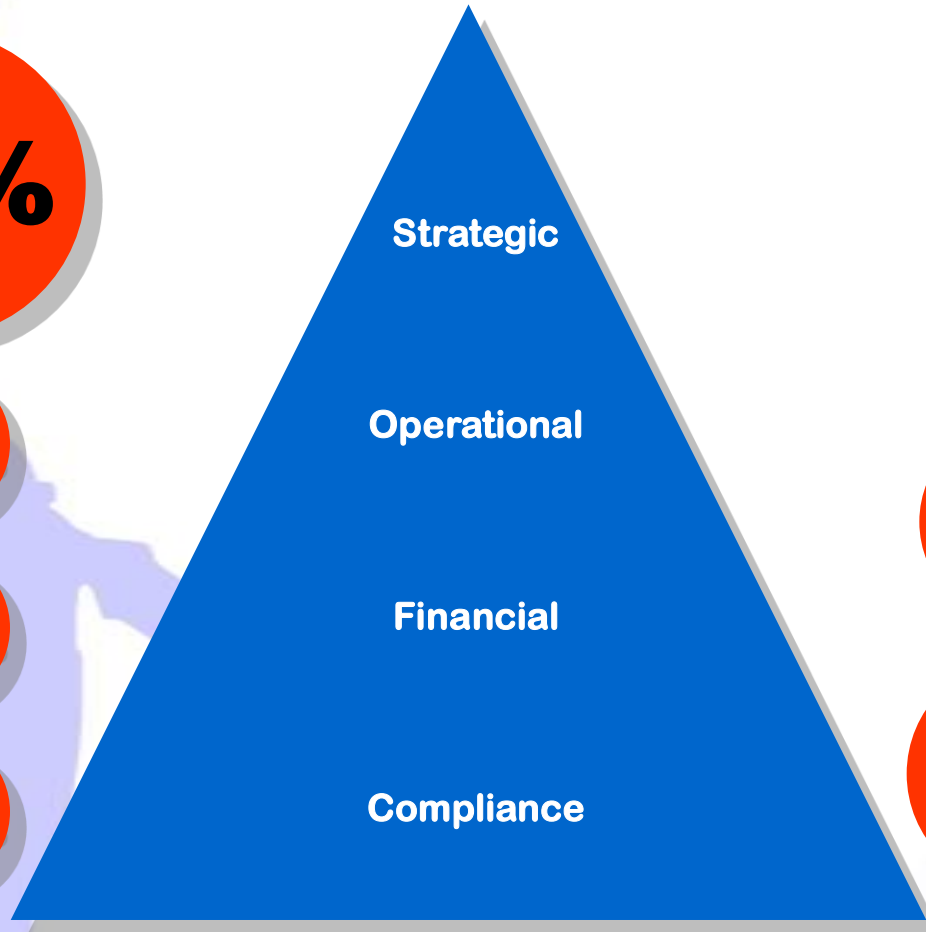
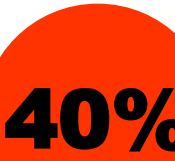


# Assurance (cont.)

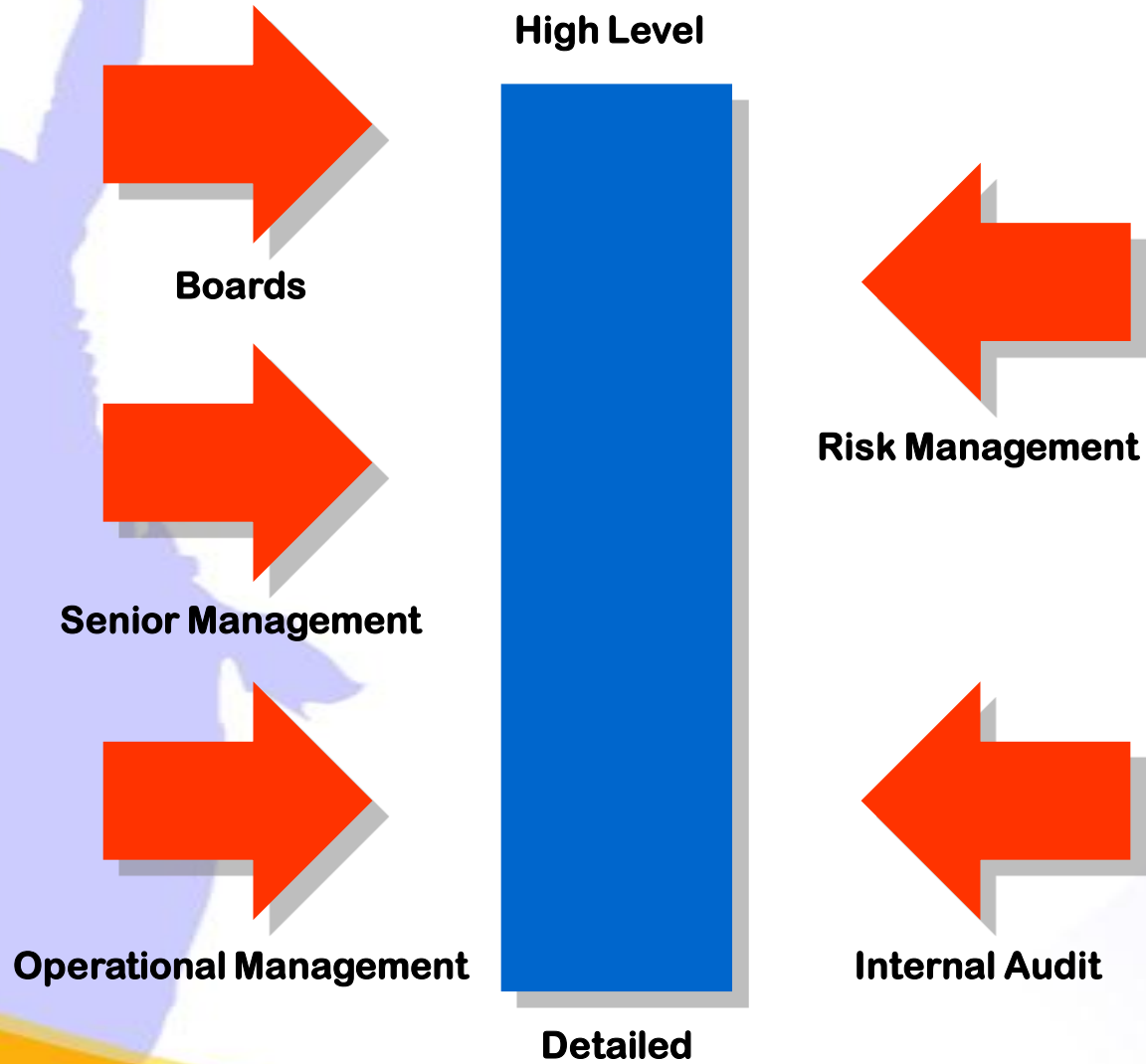
Management



Internal Audit



# Assurance (cont.)



# Assurance (cont.)

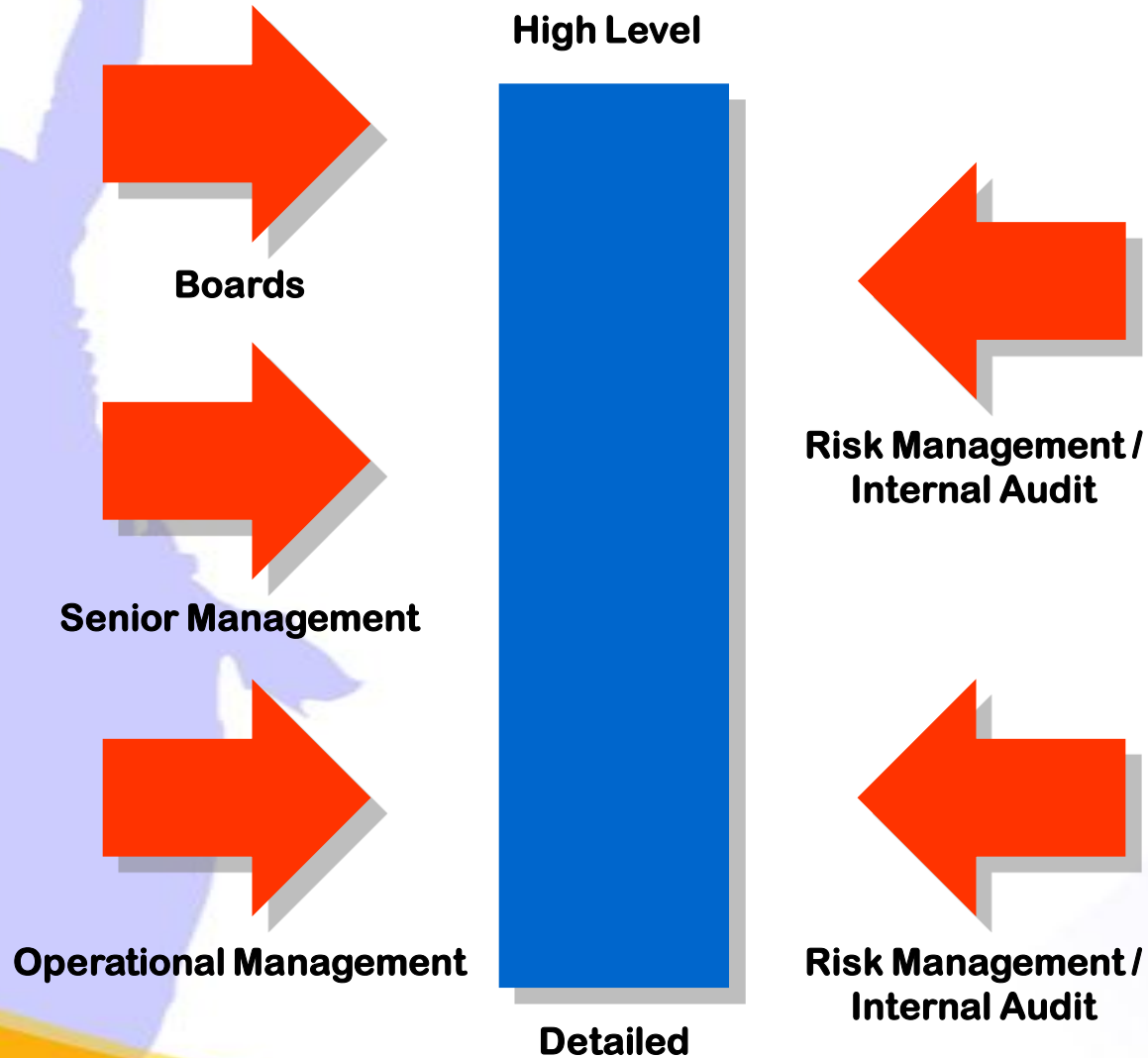


©2011 FreeBigPictures.com

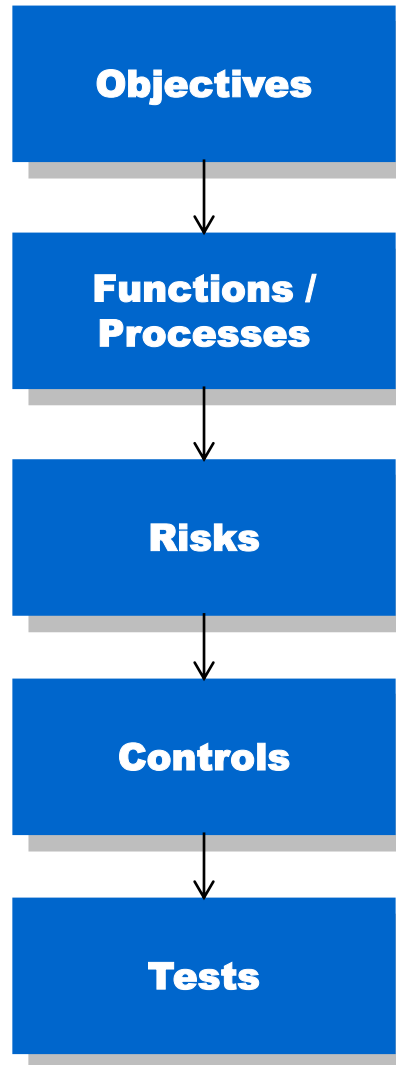




# Assurance (cont.)



# Again, let's recap . . . . .



# Risk Management

- **Process to manage risks within organisation**

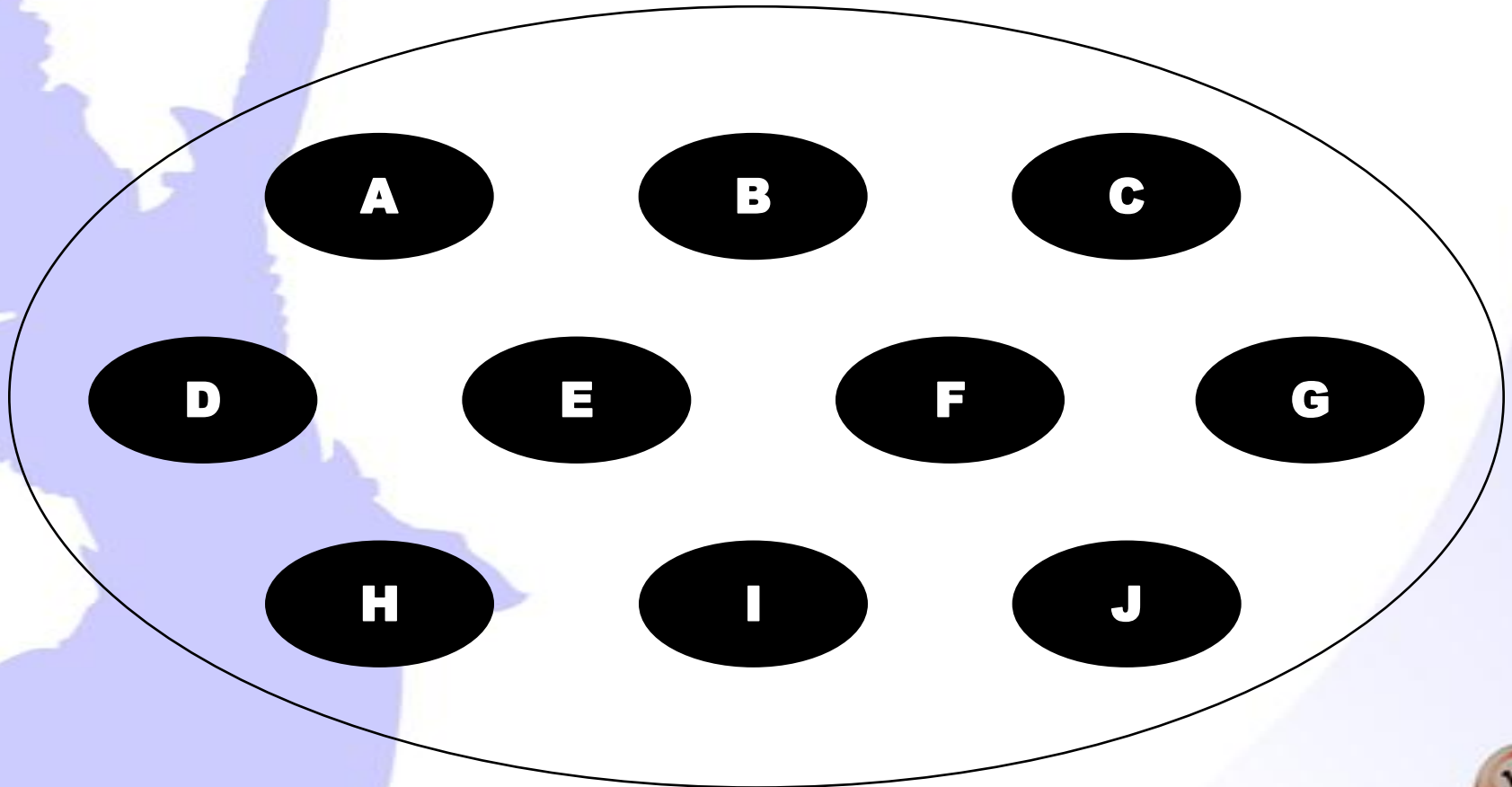


# **Risk Management (cont.)**

**If you can't measure it,  
you can't manage it**



# Risk Management (cont.)



# Risk Management (cont.)

## Risk Identification

- **For each objective, identify functions / processes that support this objective**
- **For these functions / processes, identify risks that might affect this objective**
- **Assess these risks**
- **Measure level of inherent risk**

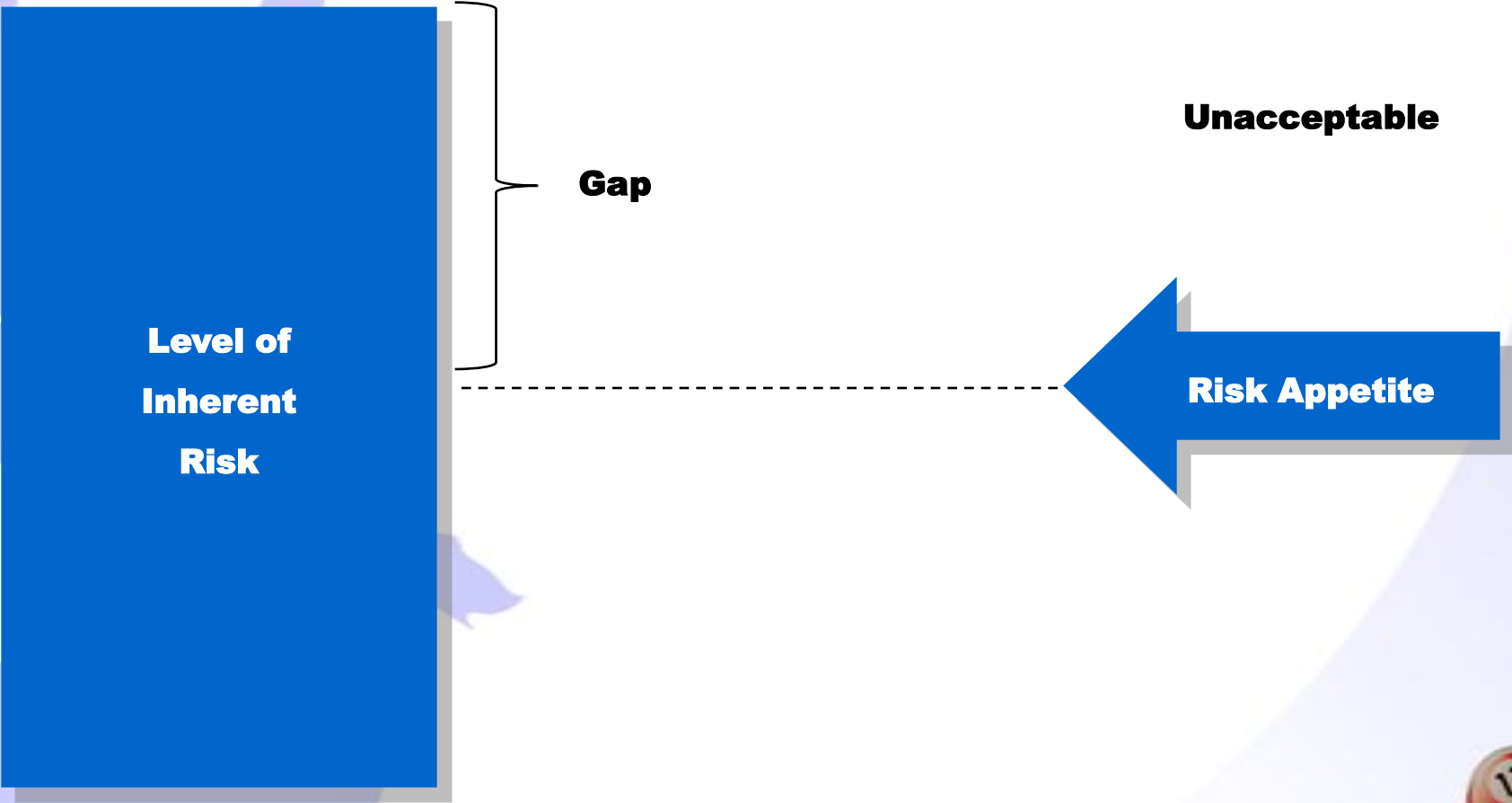


# Risk Management (cont.)

- **Risk appetite is amount of risk that management is willing to accept**

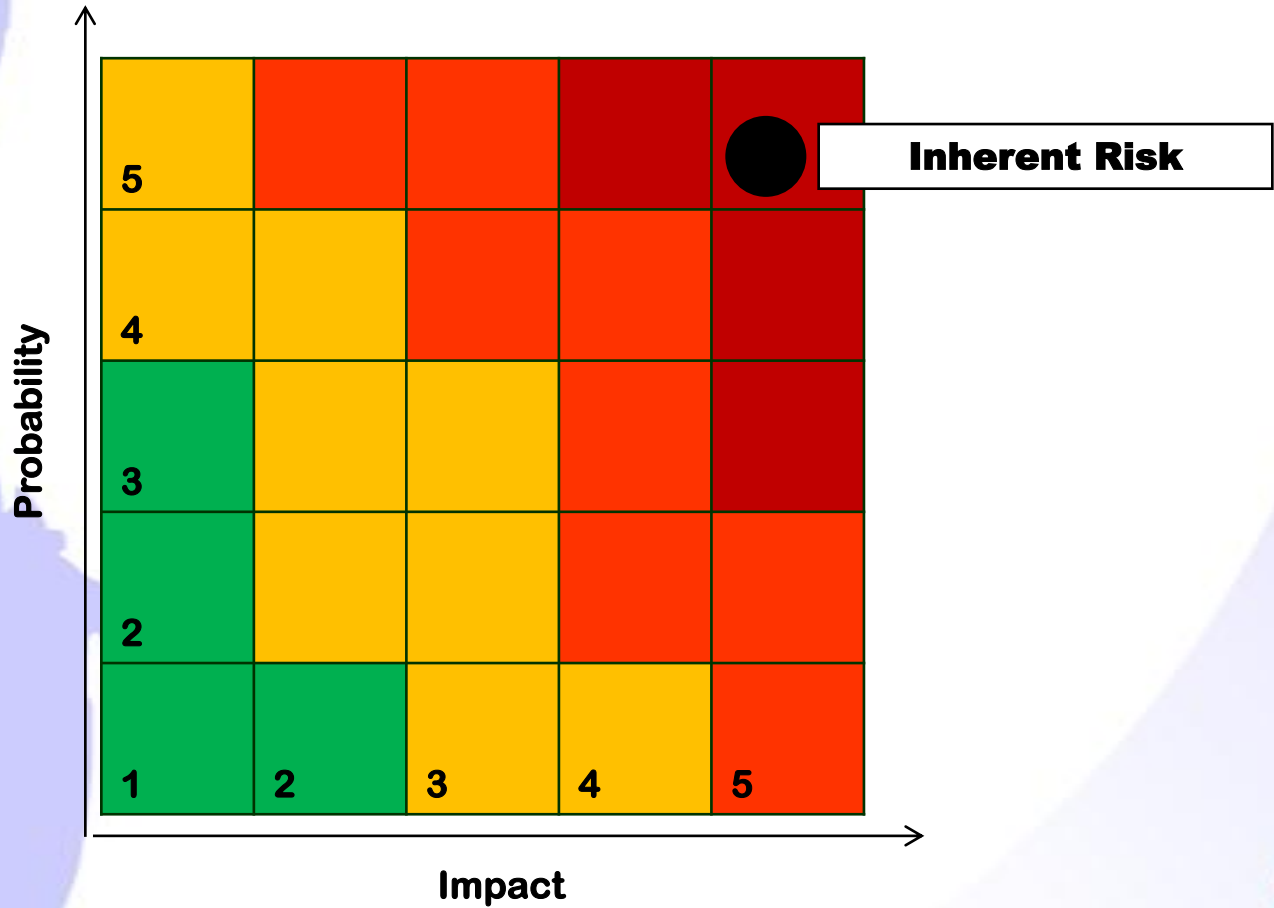


# Risk Management (cont.)

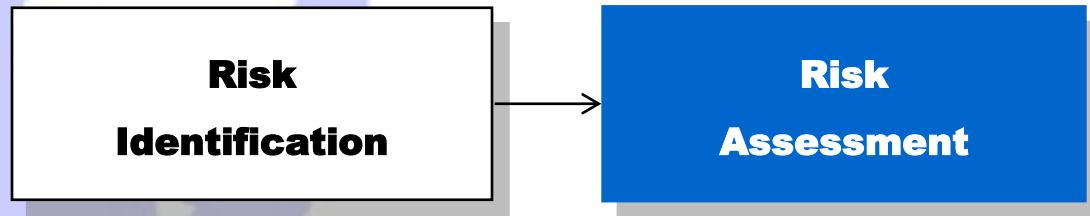




# Risk Management (cont.)



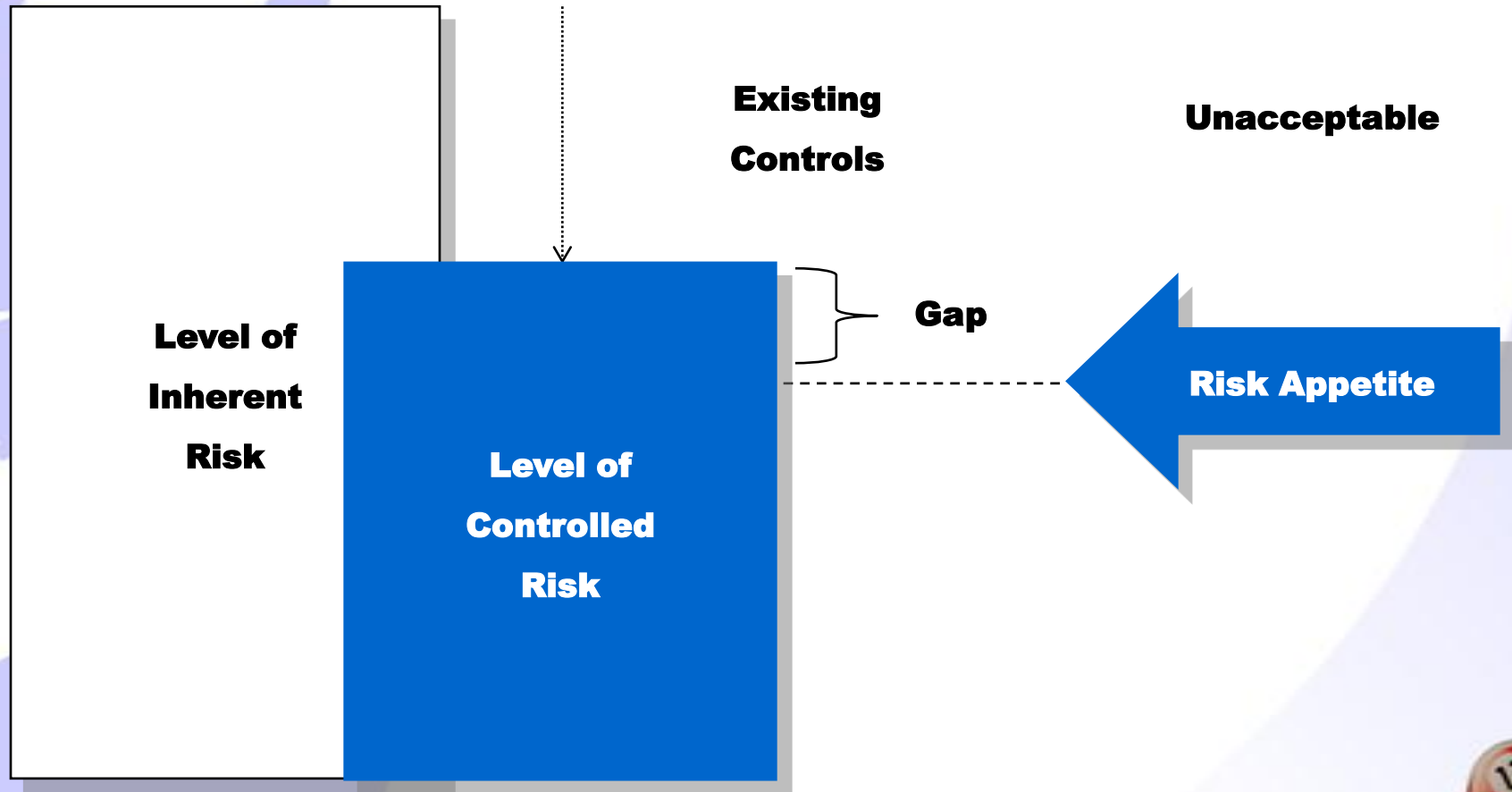
# Risk Management (cont.)



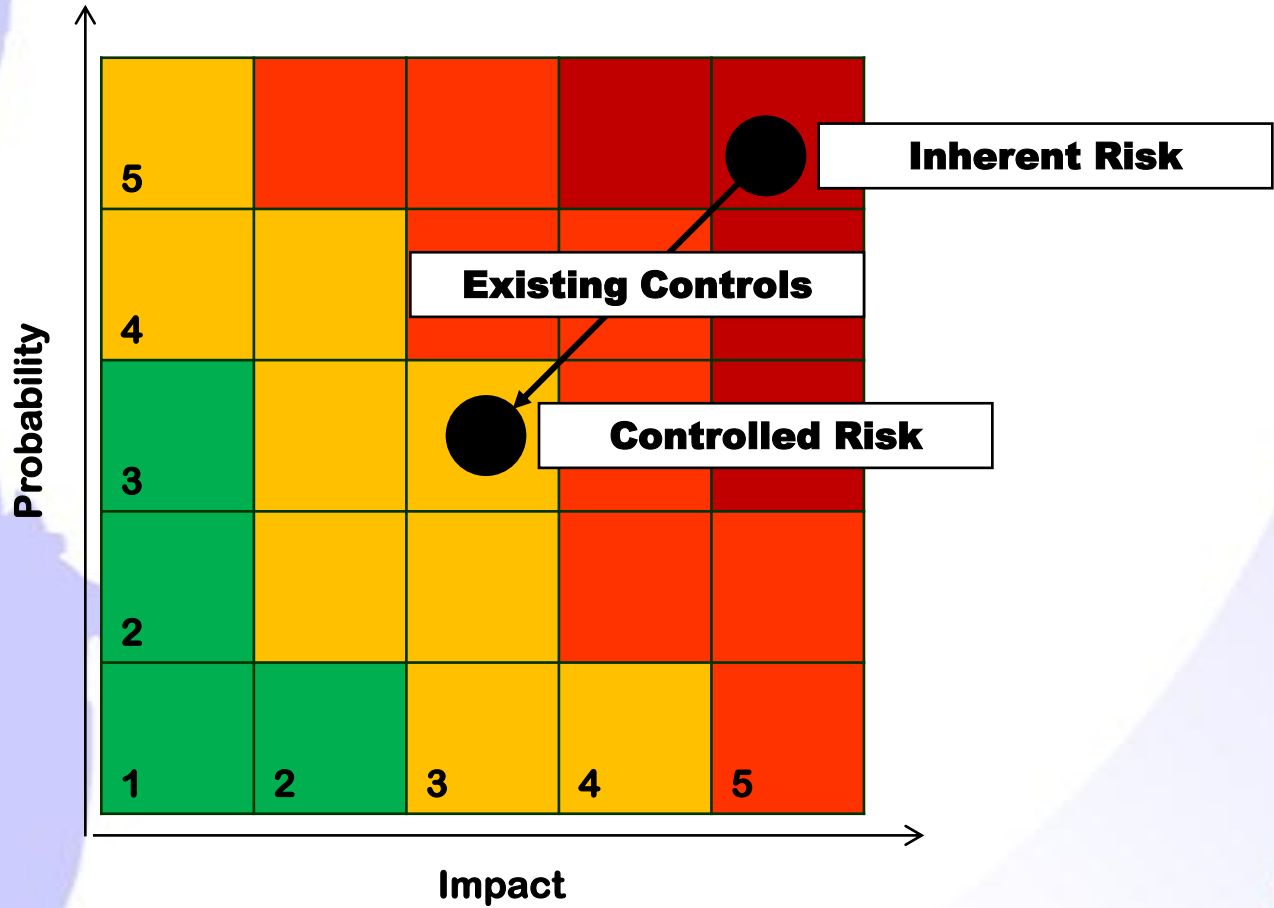
- **For these risks, assess controls that prevent, detect, and correct these risks**
- **Measure level of controlled risk**



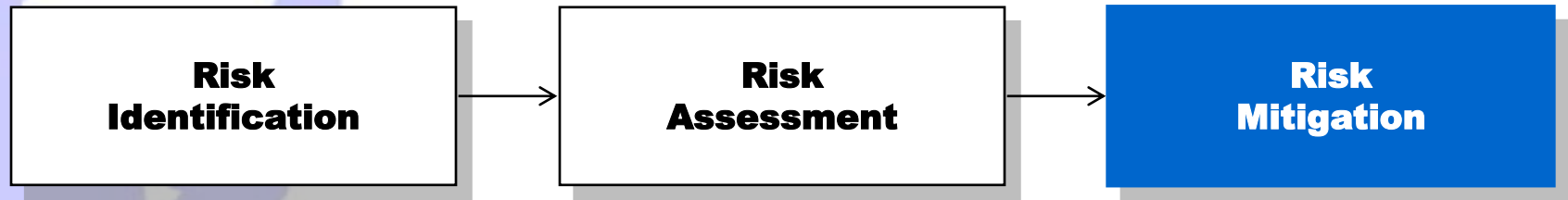
# Risk Management (cont.)



# Risk Management (cont.)



# Risk Management (cont.)



- **If level of controlled risk exceeds risk appetite, design risk responses to further reduce level of risk**
- **Measure level of residual risk**

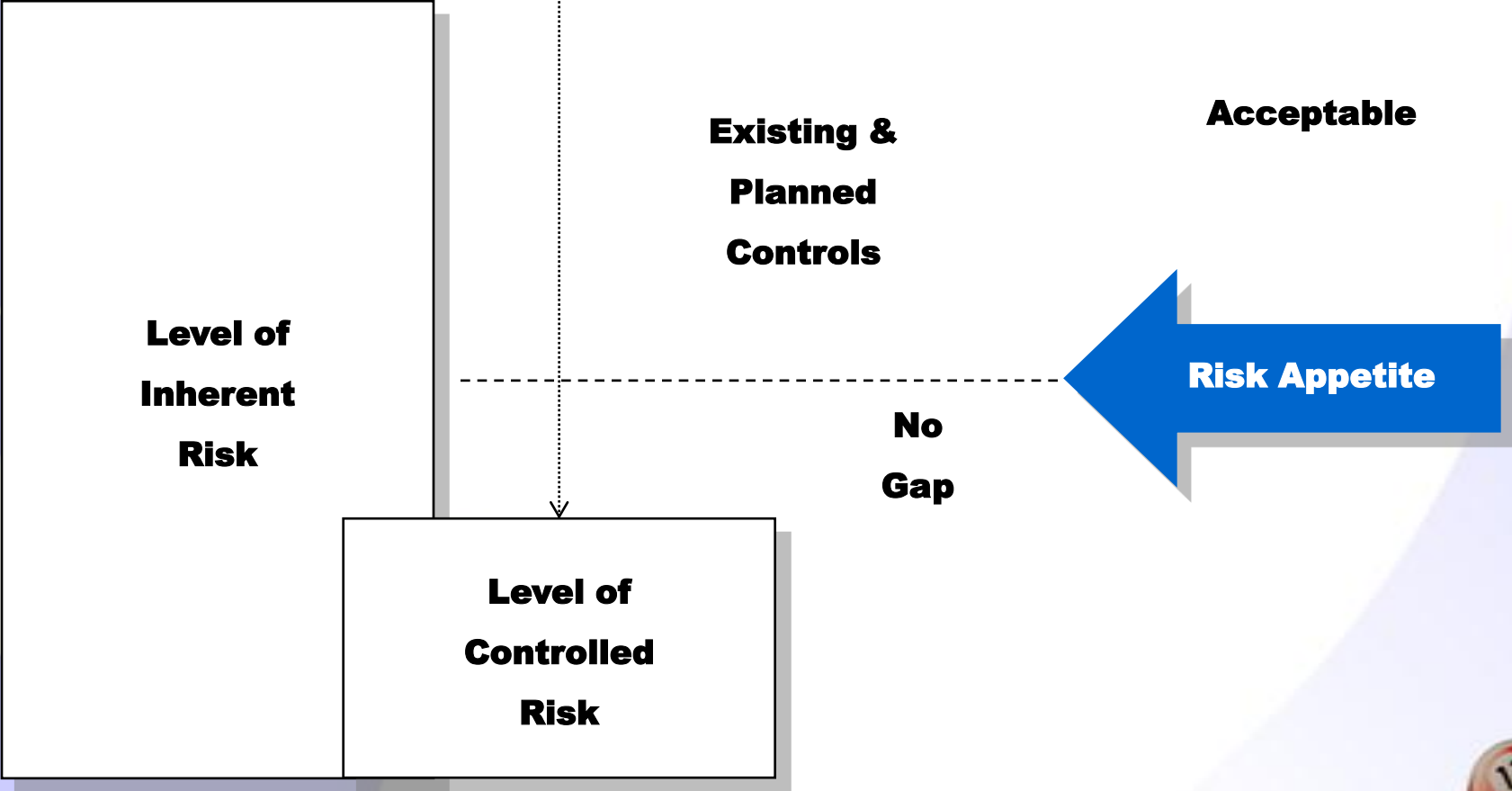


# **Risk Management (cont.)**

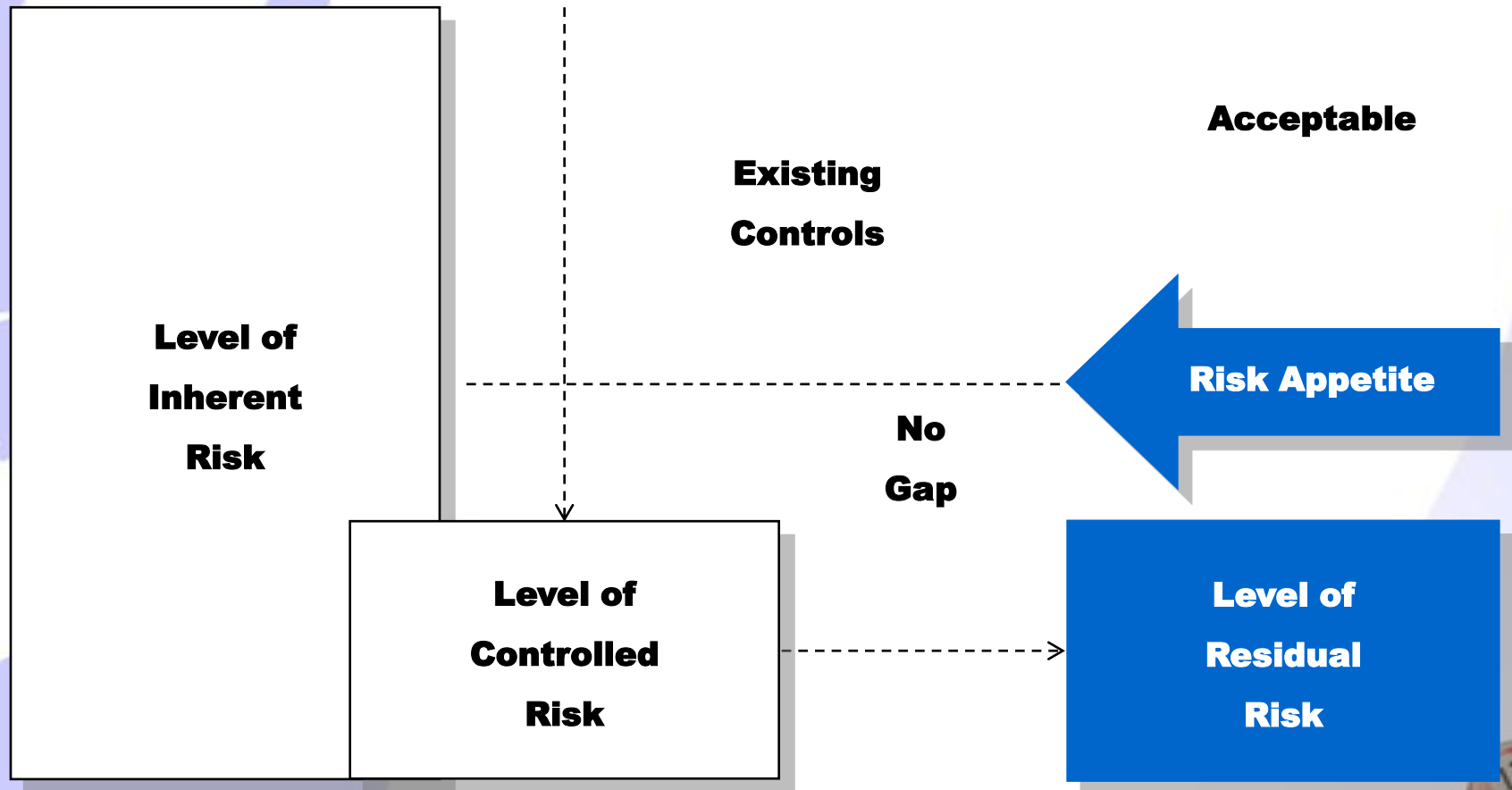
- **Terminate risk**
- **Treat impact and / or probability of risk**
- **Transfer risk via insurance, out-sourcing, etc.**
- **Tolerate risk**



# Risk Management (cont.)

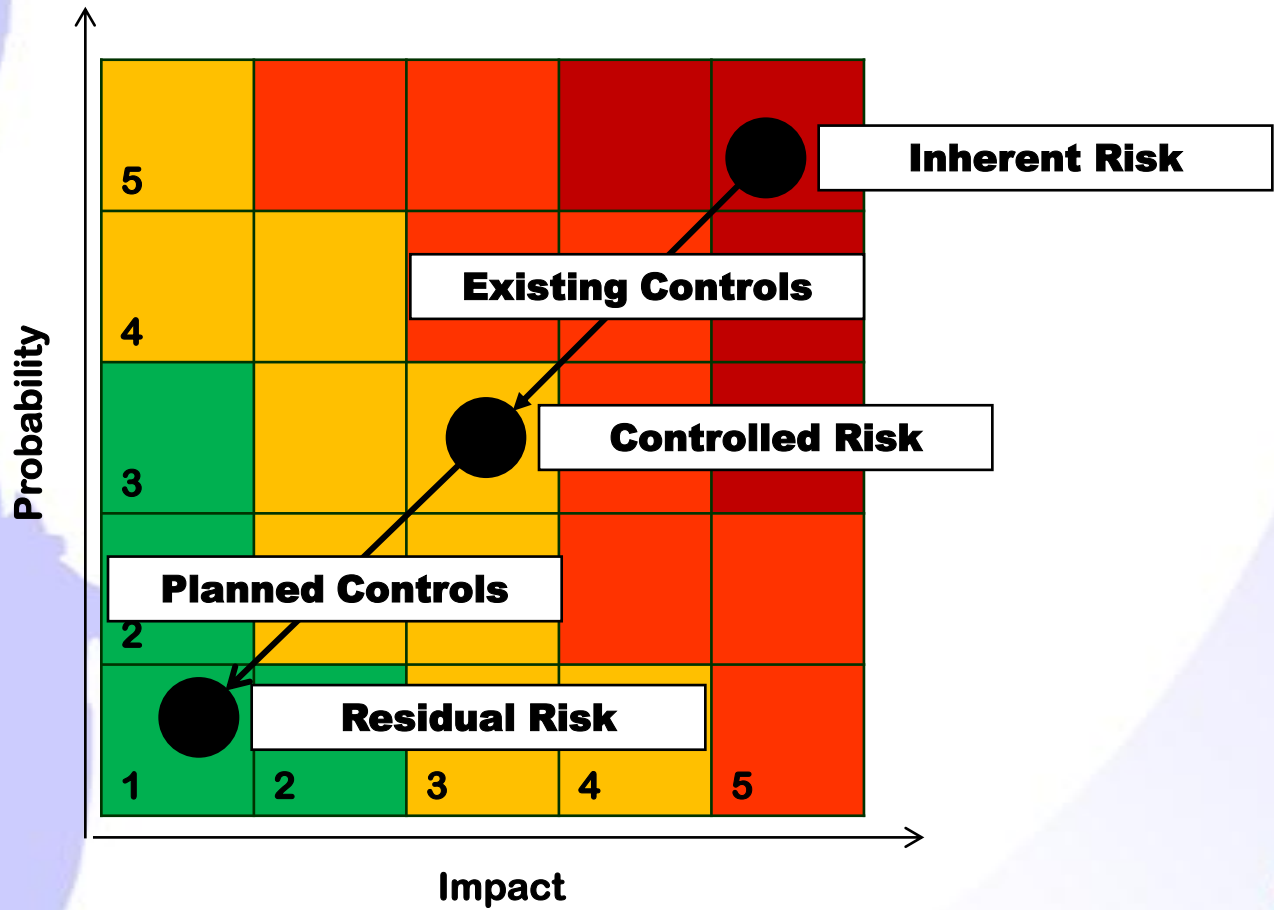


# Risk Management (cont.)

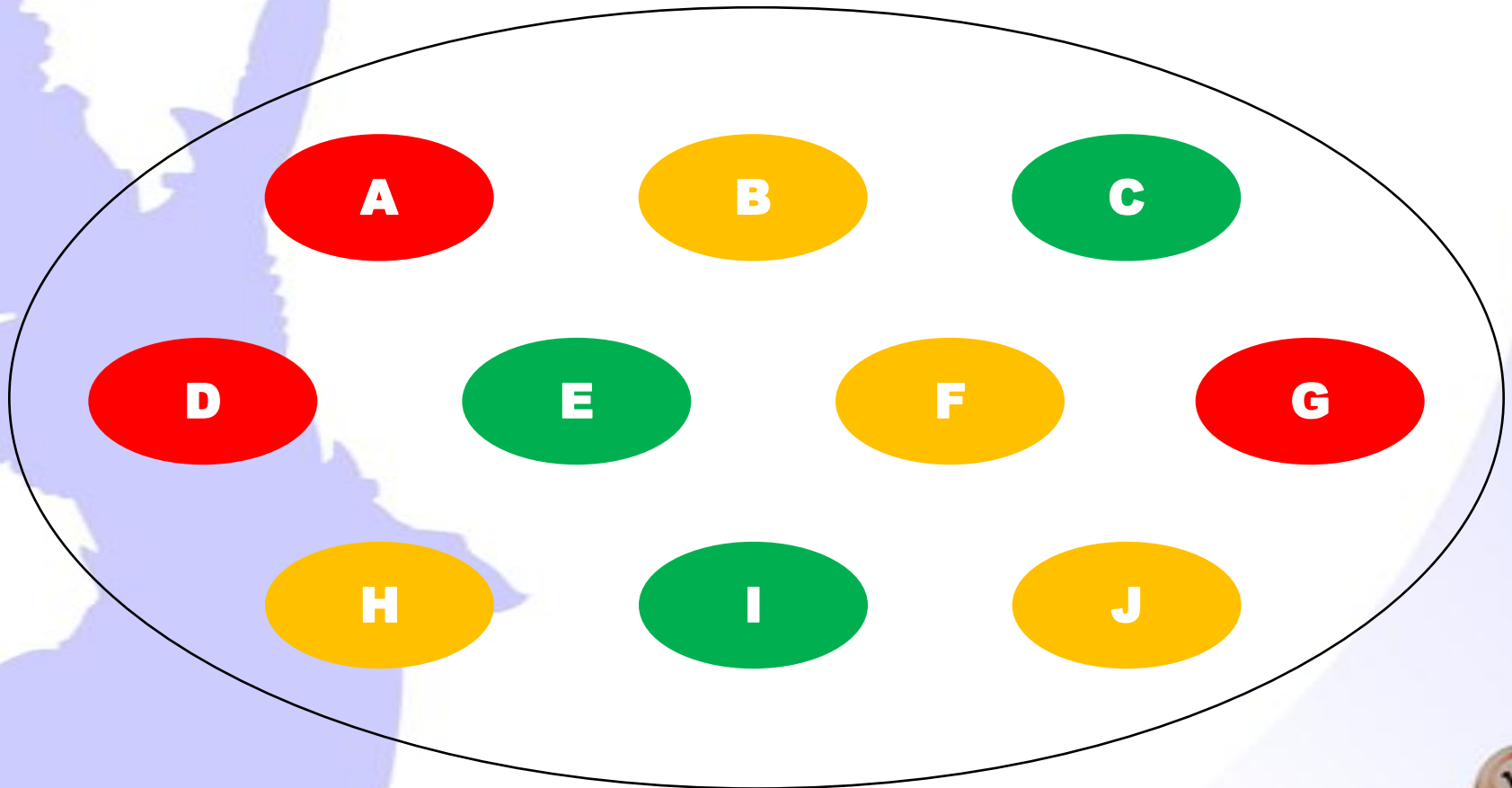











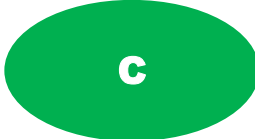


# Risk Management (cont.)



# Risk Management (cont.)

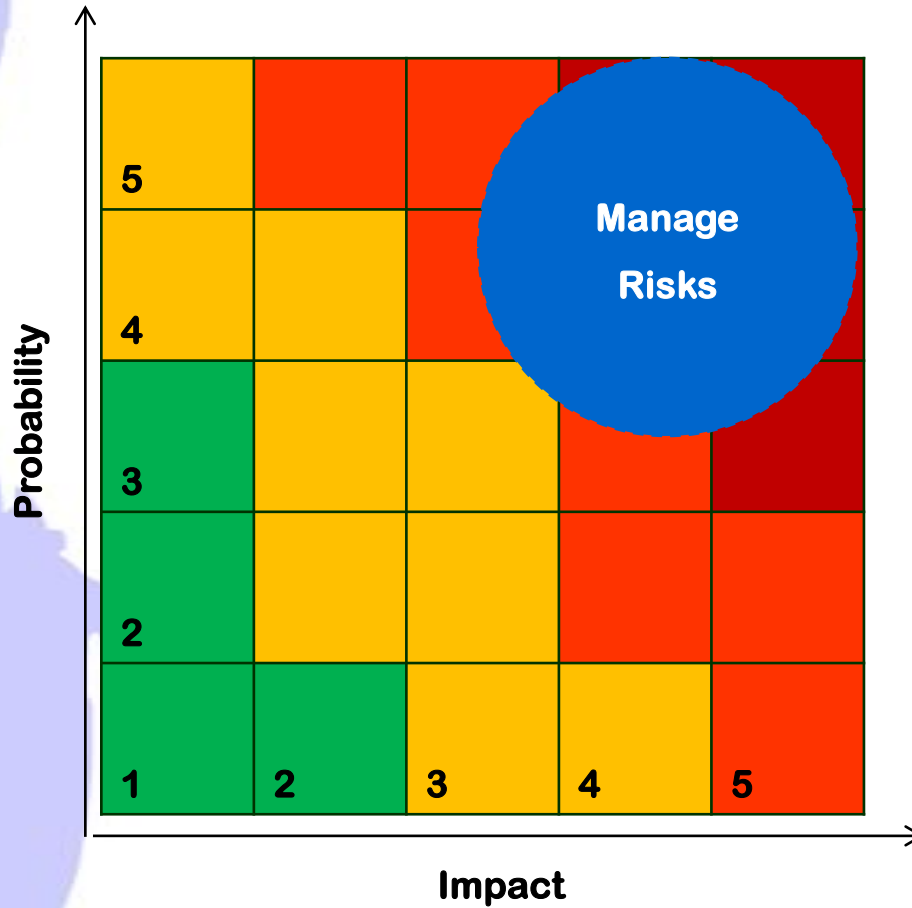


# Risk Management (cont.)

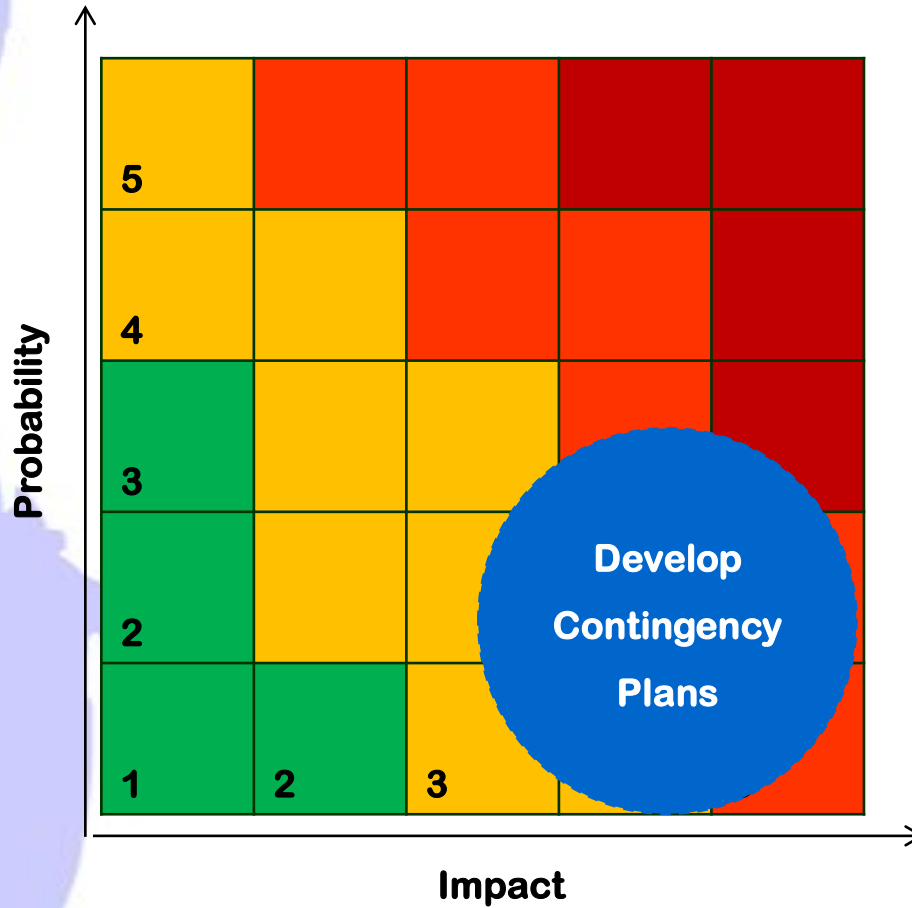
High Risk	Medium Risk	Low Risk
 <p data-bbox="382 519 428 554"><b>A</b></p>  <p data-bbox="382 676 428 711"><b>D</b></p>  <p data-bbox="382 833 428 868"><b>G</b></p>	 <p data-bbox="938 525 985 559"><b>B</b></p>  <p data-bbox="938 682 985 716"><b>E</b></p>  <p data-bbox="938 839 985 873"><b>H</b></p>  <p data-bbox="938 996 985 1031"><b>J</b></p>	 <p data-bbox="1499 519 1545 554"><b>C</b></p>  <p data-bbox="1499 676 1545 711"><b>F</b></p>  <p data-bbox="1499 833 1545 868"><b>I</b></p>



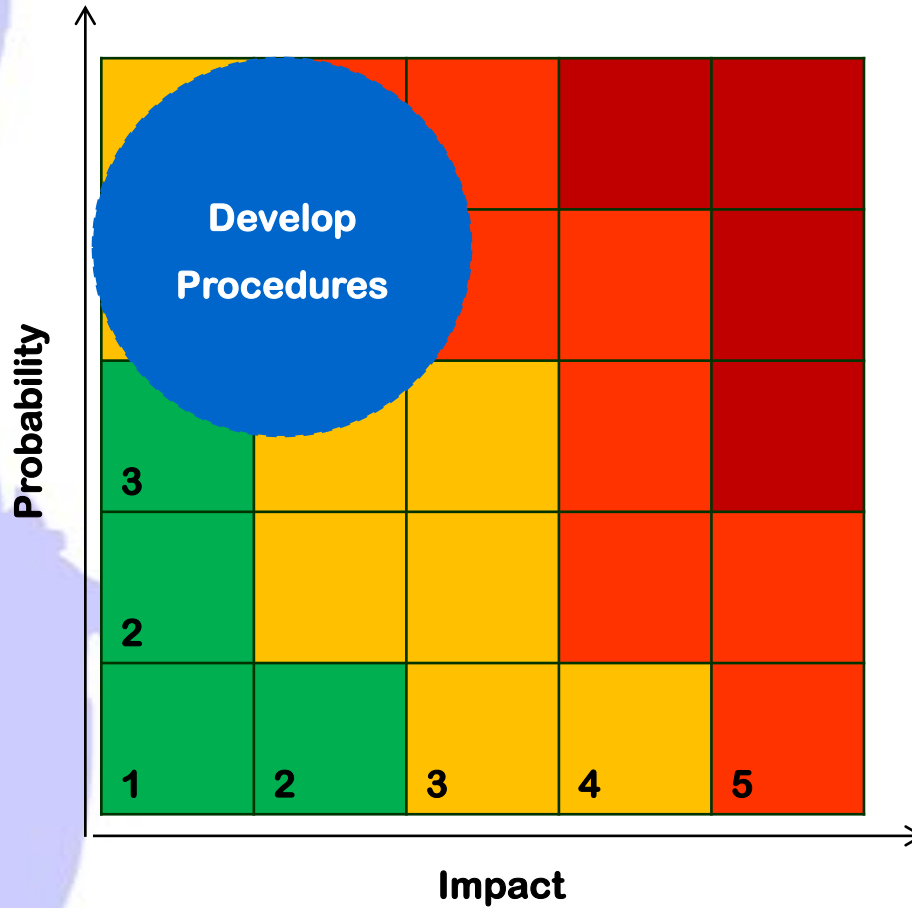
# Risk Management (cont.)



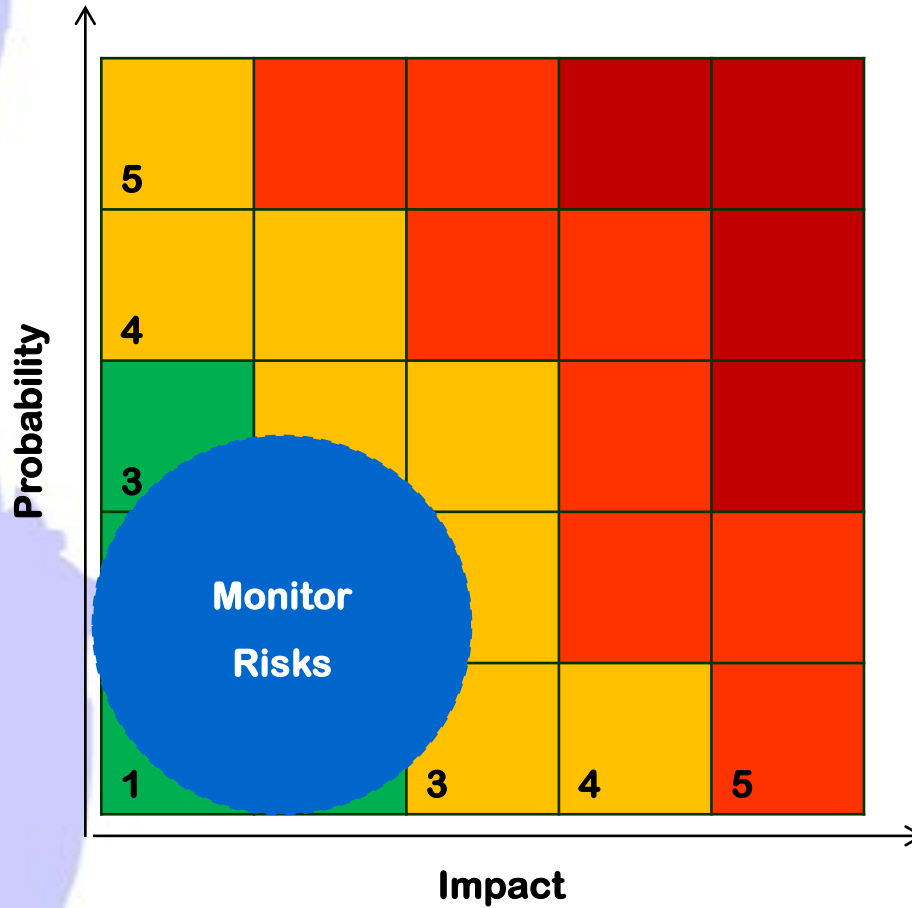
# Risk Management (cont.)



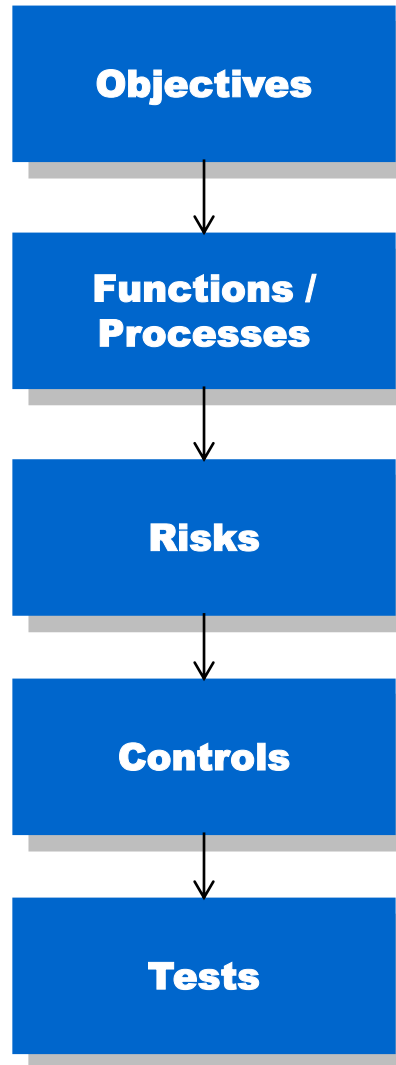
# Risk Management (cont.)



# Risk Management (cont.)



# Again, let's recap . . . . .





# Internal Audit

- **Internal auditing is independent, objective assurance and consulting activity designed to add value and improve organisation's operations**
- **It helps organisation accomplish its objectives by bringing systematic, disciplined approach to evaluate and improve effectiveness of governance, risk management and control processes**

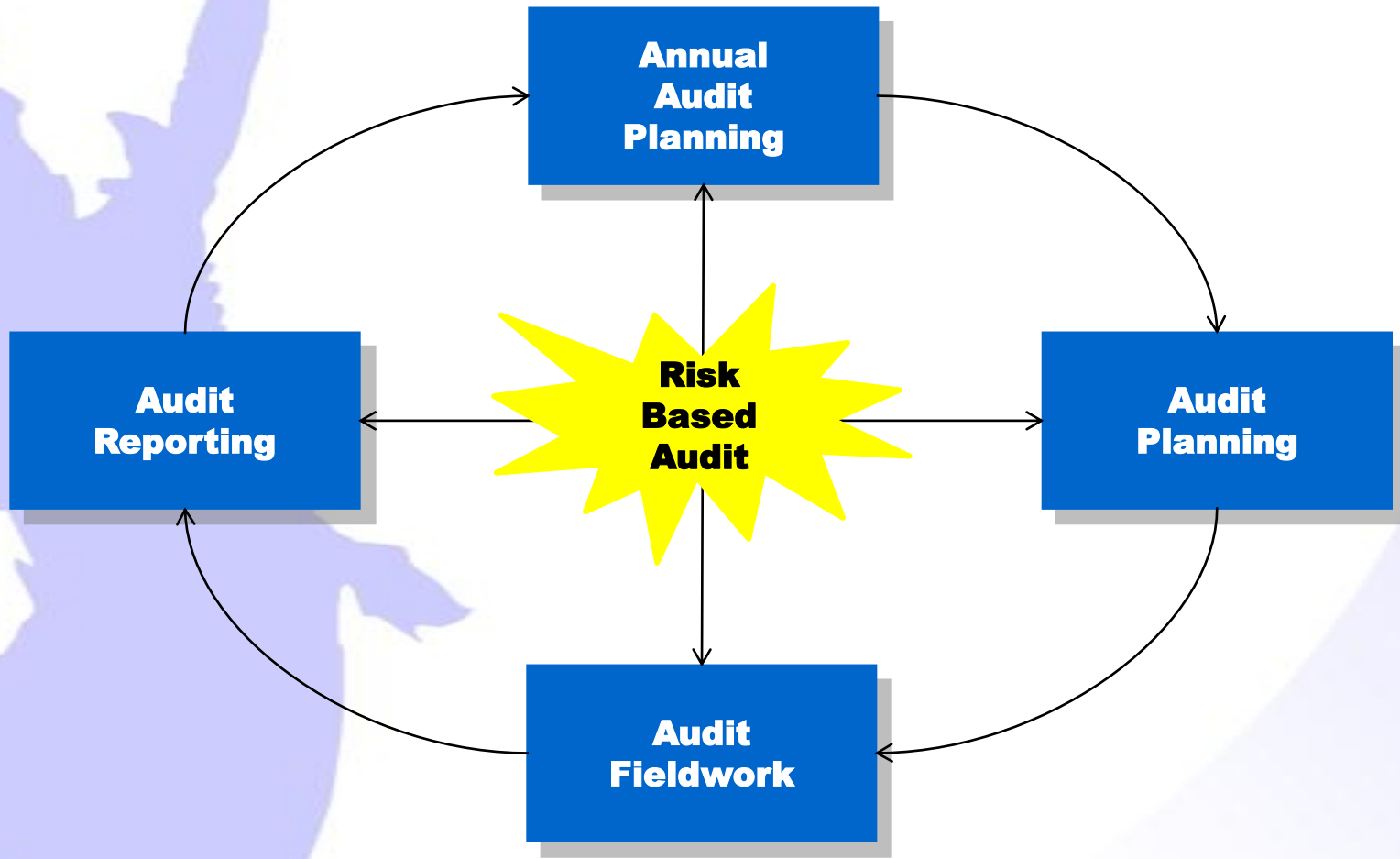


# Internal Audit (cont.)

- **Annual audit planning**
- **Audit planning**
- **Audit fieldwork**
- **Audit reporting**
- **Audit follow-up**



# Internal Audit (cont.)



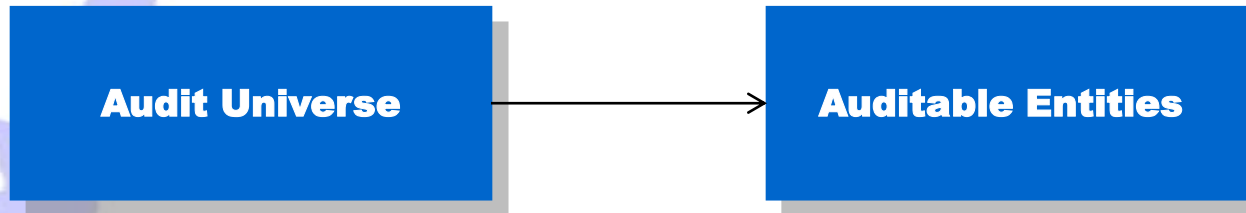
# **Internal Audit (cont.)**

## **Annual Audit Planning**

- **Annual plans should be developed based upon macro-risk assessment**



# Internal Audit (cont.)

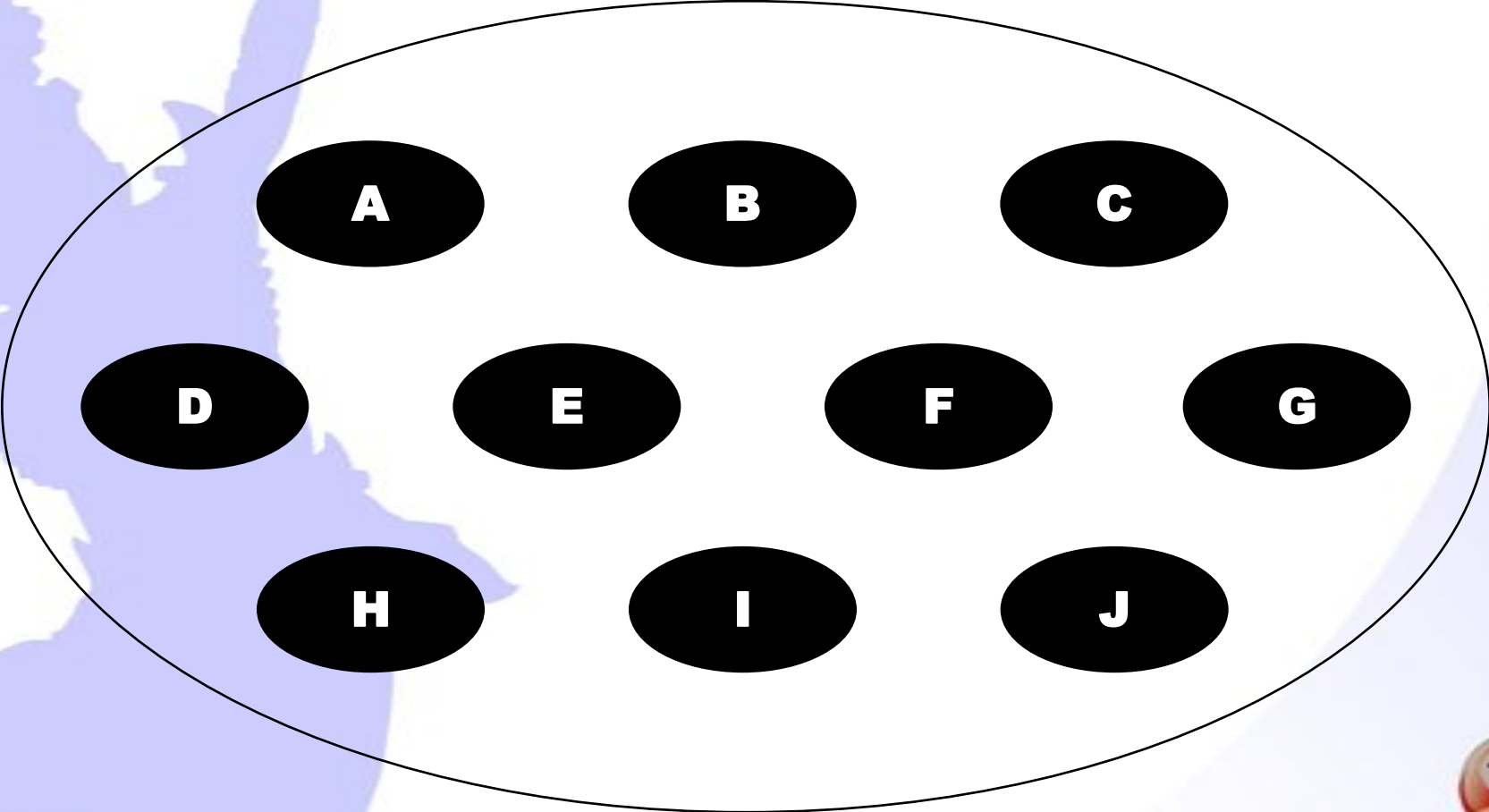


# Internal Audit (cont.)

- **Objectives**
- **Functions**
- **Processes**
- **Others**



# Internal Audit (cont.)



# Internal Audit (cont.)

- **Risk factors**
- **Specific risks**





# Internal Audit (cont.)

## Risk Factors

- **For each auditable entity:**
  - **Determine risk factors**
  - **Determine weightings**
  - **Assign scores**
  - **Calculate risk scores**
  - **Assign risk levels**



# Internal Audit (cont.)

## Risk Factors (cont.)

<b>Risk Factors</b>	<b>Weightings</b>	<b>Scores</b>	<b>Totals</b>
▪ <b>Factor A</b>	<b>0.5</b>	<b>8</b>	<b>4</b>
▪ <b>Factor B</b>	<b>0.25</b>	<b>10</b>	<b>2.5</b>
▪ <b>Factor C</b>	<b>0.25</b>	<b>3</b>	<b>0.75</b>
<b>Grand Total</b>			<b>7.25</b>



# Internal Audit (cont.)

## Risk Factors (cont.)

- **Convert grand total to risk level:**
  - **High risk : 7 - 10**
  - **Medium risk : 4 - 6**
  - **Low risk : 1 - 3**



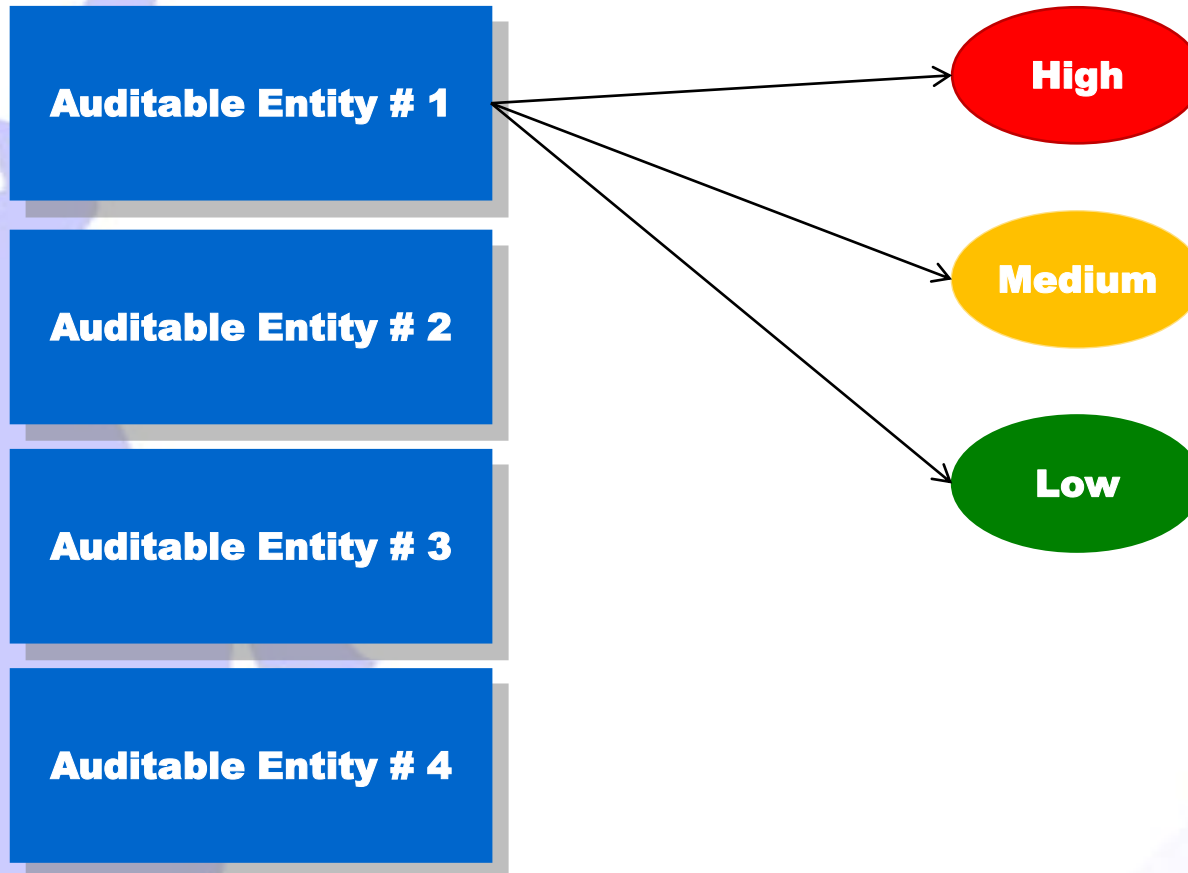
# Internal Audit (cont.)

## Risk Factors (cont.)

<b>Risk Factors</b>	<b>Weightings</b>	<b>Scores</b>	<b>Totals</b>
▪ <b>Factor A</b>	<b>0.5</b>	<b>8</b>	<b>4</b>
▪ <b>Factor B</b>	<b>0.25</b>	<b>10</b>	<b>2.5</b>
▪ <b>Factor C</b>	<b>0.25</b>	<b>3</b>	<b>0.75</b>
<b>Grand Total</b>			<b>7.25</b>



# Internal Audit (cont.)



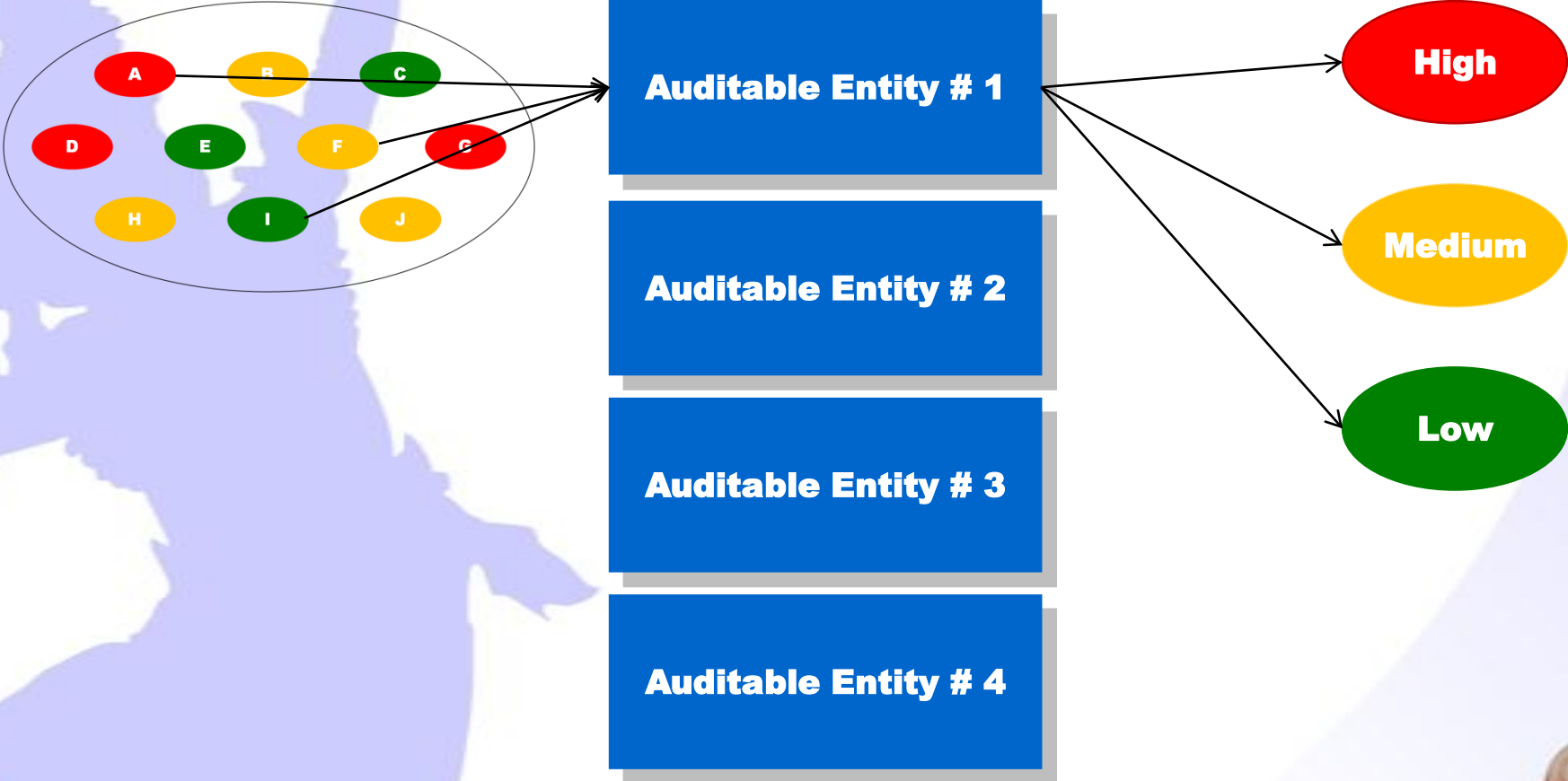
# Internal Audit (cont.)

## Specific Risks








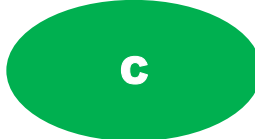


- **For each auditable entity:**
  - **Link specific risks**
  - **Summarise risks levels**



# Internal Audit (cont.)



# Internal Audit (cont.)

High Risk	Medium Risk	Low Risk
  	   	  





# Internal Audit (cont.)

- **Determine approach**
- **Determine effort**
- **Determine frequency**



# Internal Audit (cont.)

## Audit Planning

- **Audits should be planned based upon micro-risk assessment, potentially using those risks identified through risk management**



# Internal Audit (cont.)

## Audit Fieldwork

- **Audits should be completed based upon micro-risk assessment**



# Internal Audit (cont.)

## Audit Reporting

- **Audits should be reported based upon micro-risk assessment**



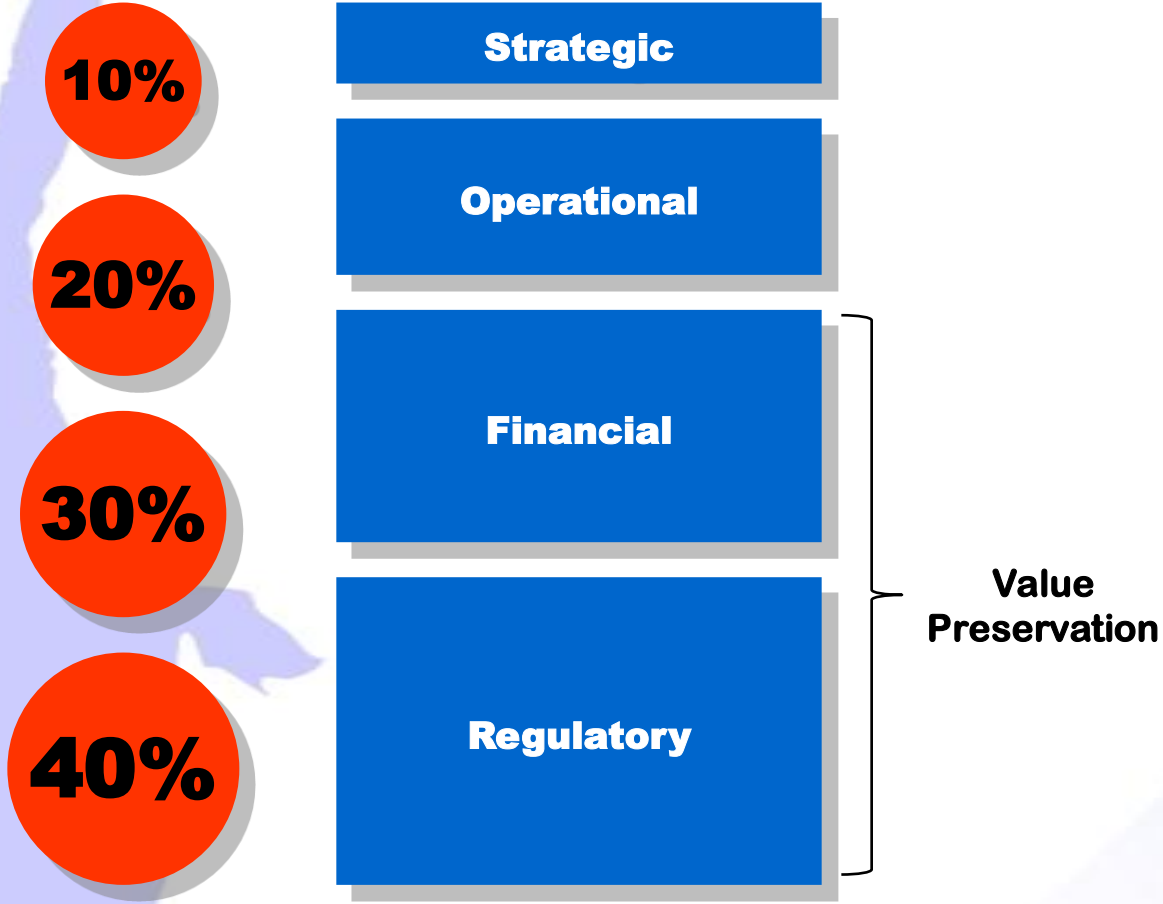
# Internal Audit (cont.)

## Audit Follow-up

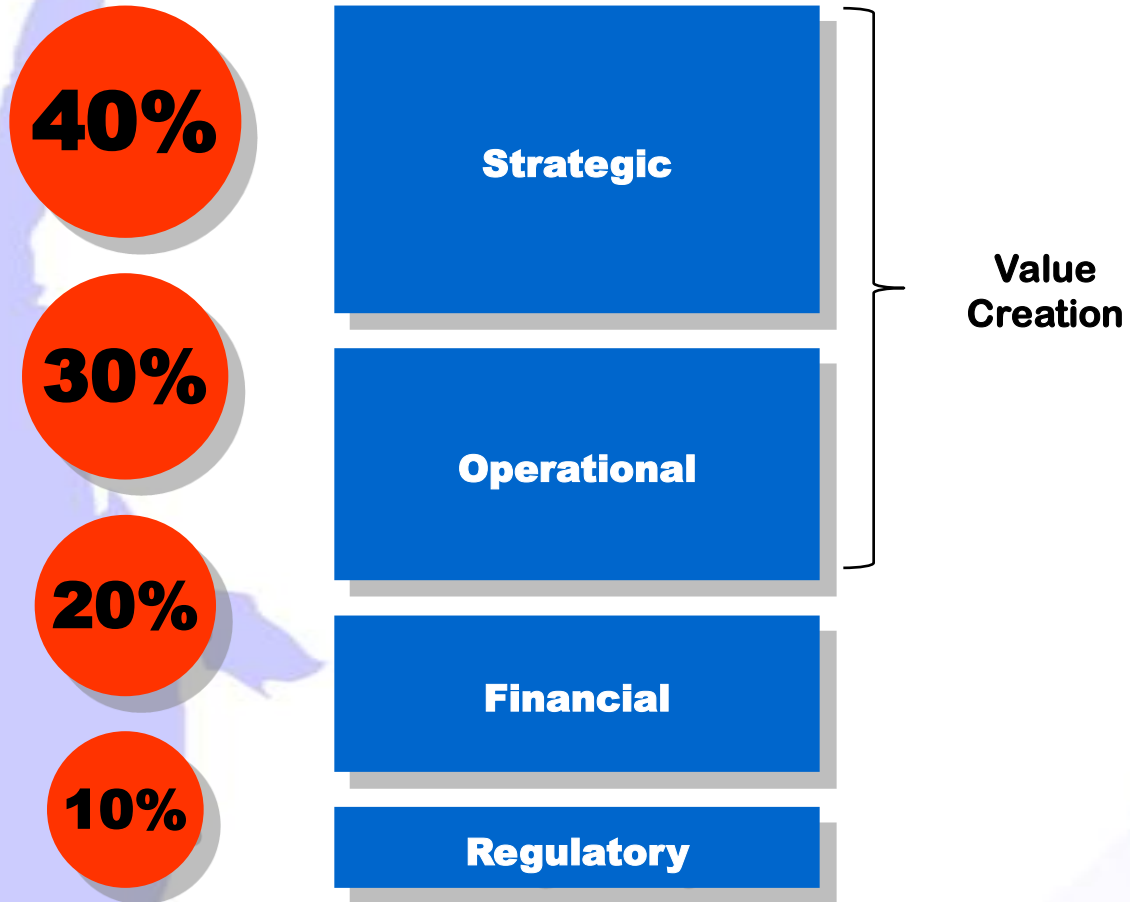
- **Audits should be followed-up based upon micro-risk assessment**



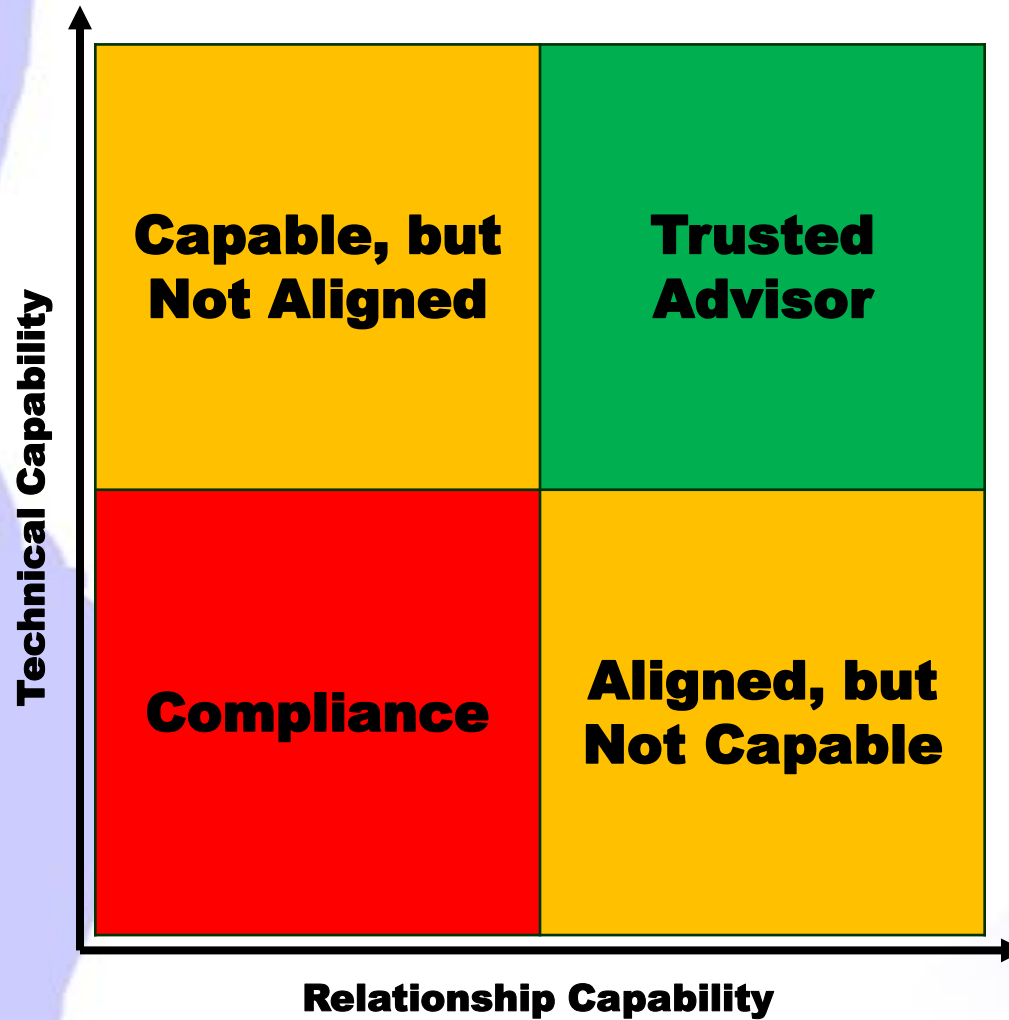
# Conclusion



# Conclusion (cont.)



# Conclusion (cont.)





# Conclusion (cont.)

- **Phil Leifermann**
- **Managing Director, Insight Consulting**
- **Mobile : +61 488 765-711 / +62 811 890-829**
- **Email : [phil.leifermann@insight.co.id](mailto:phil.leifermann@insight.co.id)**

