Garry Barnes
Vice President, **ISACA**
Practice Lead, Governance Advisory, **Vital Interacts**

VALUE CREATION THROUGH OPTIMISING RISK

December 2014

BACKGROUND

ISACA:

International Vice President

Treasurer, Finance Committee

Strategic Advisory Council

Credentialing and Career Management Board

CISM Certification Committee (Chair) and TES

Oceania CACS Committees (2004, 2008, 2015)

Sydney Chapter 2003-2012 (President 2008-10)

Security, Governance, Risk and Audit:

Practice Lead, Governance Advisory, Vital Interacts

Managing Consultant, BAE Systems

Risk Manager & Information Security Consultant, Commonwealth Bank of Australia

Information Security Manager & IT Audit Manager, NSW Departments of Education & Commerce

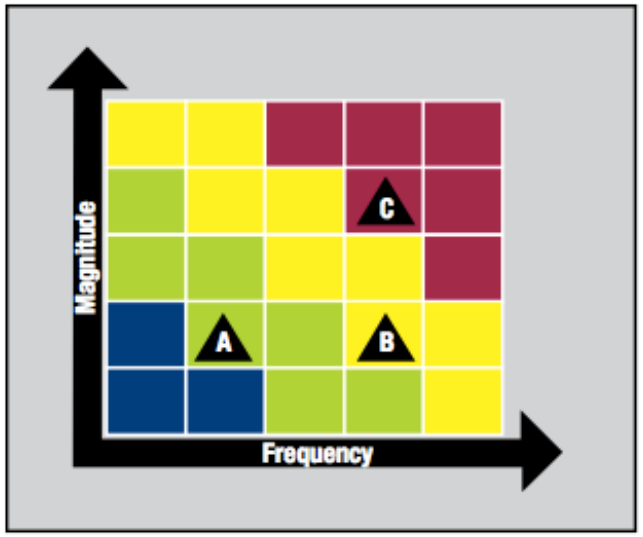
CISA CISM CGEIT CRISC MAICD

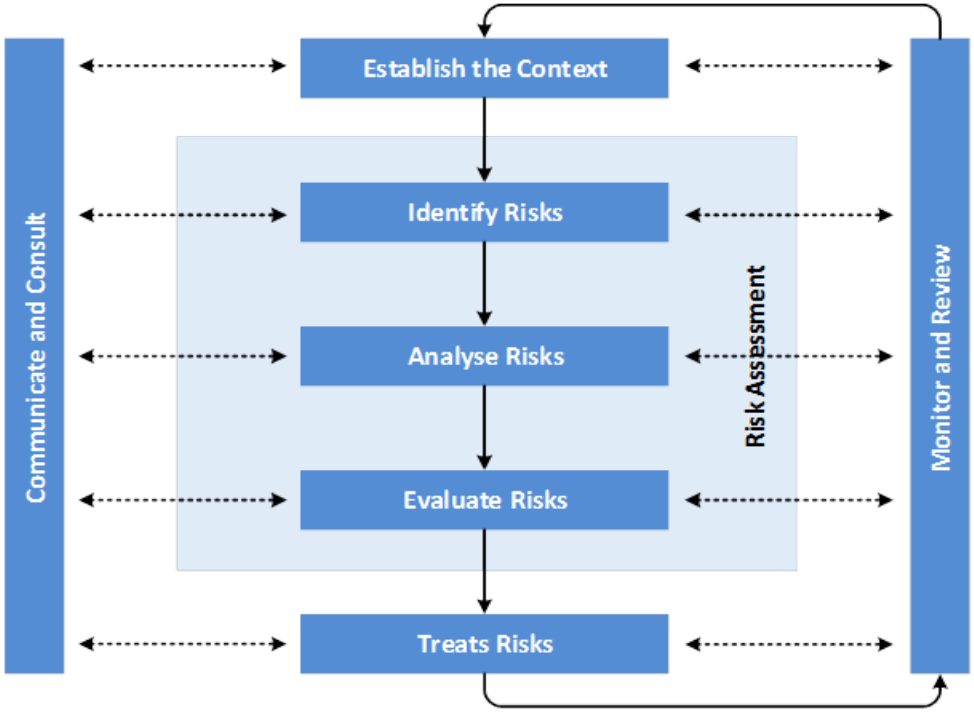
ISACA®
Trust in, and value from, information systems

COMMON APPROACHES

Risk: the likelihood that a loss will occur.

Risk = Threats x assets x vulnerabilities





RISK MANAGEMENT AT LOW PERFORMING ORGANISATIONS

- ✗ Is used primarily for compliance:
  - ✗ Supporting compliance reporting
  - ✗ Identifying and assessing controls to minimise breaches
- ✗ Is constrained by internal organisational boundaries
- ✗ Is reactive:
  - ✗ An additional and separate step in decision making
  - ✗ Identified risks viewed as poor performance
- ✗ Static view of risk:
  - ✗ Ignoring changing business requirements
  - ✗ Once a year risk assessment
- ✗ Ineffective risk monitoring:
  - ✗ Inaccurate measurement of actual risk levels
  - ✗ No enterprise-wide view provided by risk aggregation
- ✗ Wrong accountability model:
  - ✗ Risk Managers (or Owners) vs Risk Facilitators (or Function)

ISACA®
Trust in, and value from, information systems

RISK MANAGEMENT AT TOP PERFORMING ORGANISATIONS

- ✓ Is closely linked with strategy:
  - ✓ Risk with new products and services, Mergers and Acquisitions, etc.
- ✓ Is a proactive and consistent:
  - ✓ Risk information is available to support strategic, change and operational decisions
- ✓ Integrates Enterprise and IT risk:
  - ✓ Common language
  - ✓ Aggregation of risks
- ✓ Links with business outcomes:
  - ✓ Creates awareness and understanding of risk policy
  - ✓ Risk Appetite Statement provides a reference point leading to better business decisions

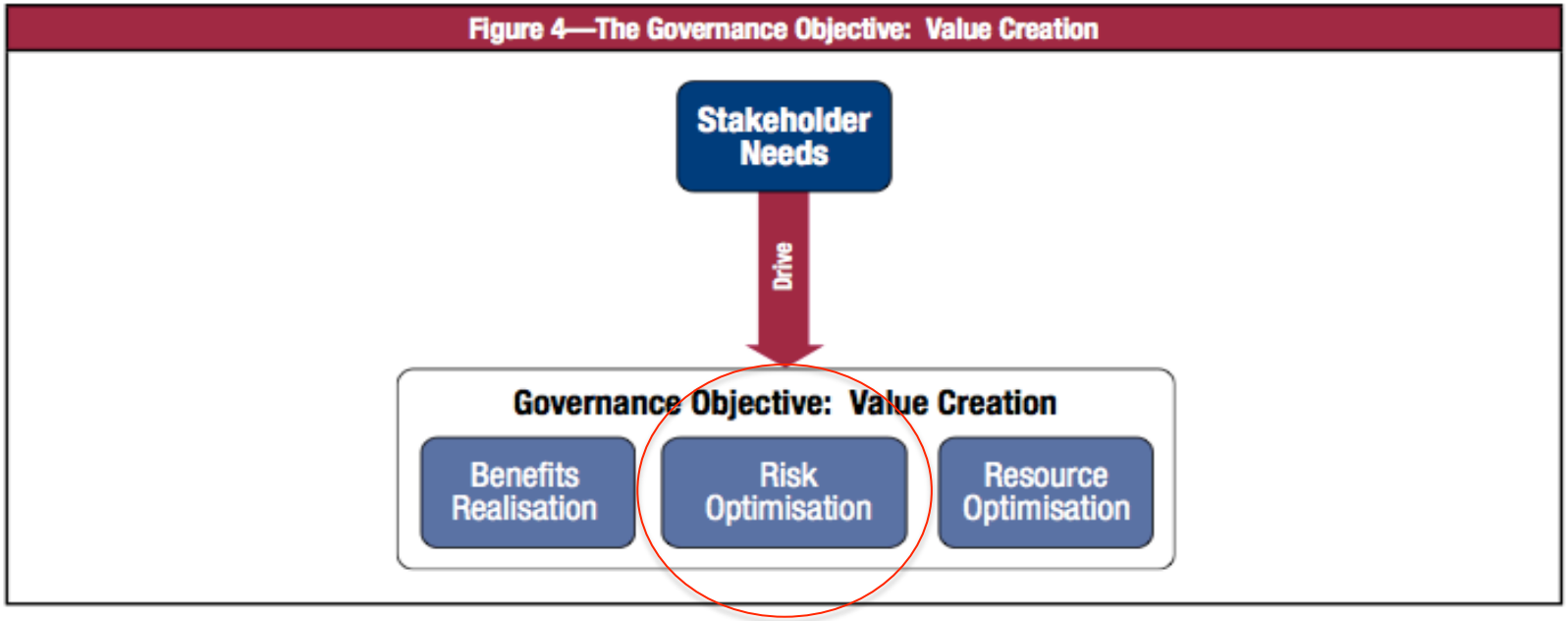
ISACA®
Trust in, and value from, information systems

COBIT 5 – "RISK OPTIMISATION"

COBIT 5
AN ISACA® FRAMEWORK

The Governance Objective:

"Value creation means realising benefits at an optimal resource cost while optimising risk"

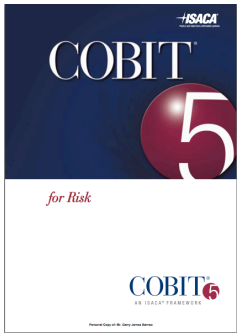


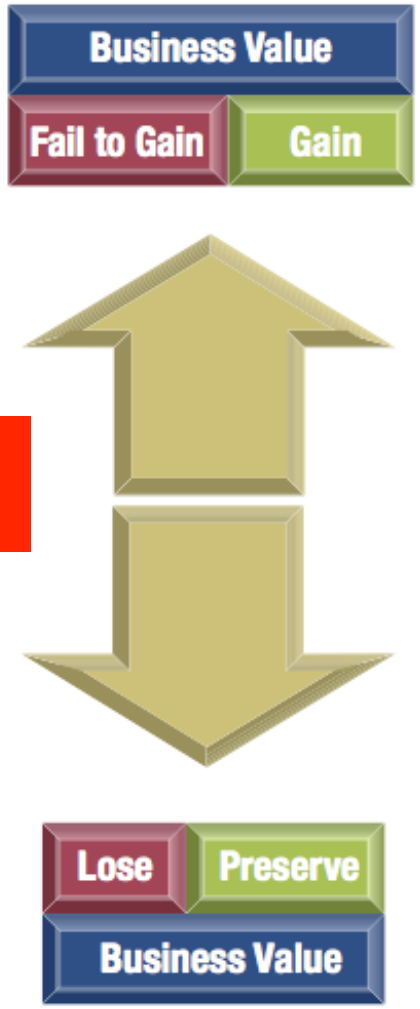
ISACA®
Trust in, and value from, information systems

NEXT STEPS FOR RISK MANAGEMENT

- **Risk and opportunity**
- Risk capability
- Risk scenarios
- Risk appetite

COBIT 5 FOR RISK – "DUALITY OF RISK"





Do things badly and lose or fail to gain value

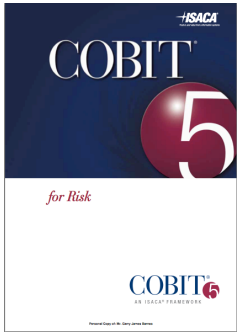
Do things well and preserve or gain value

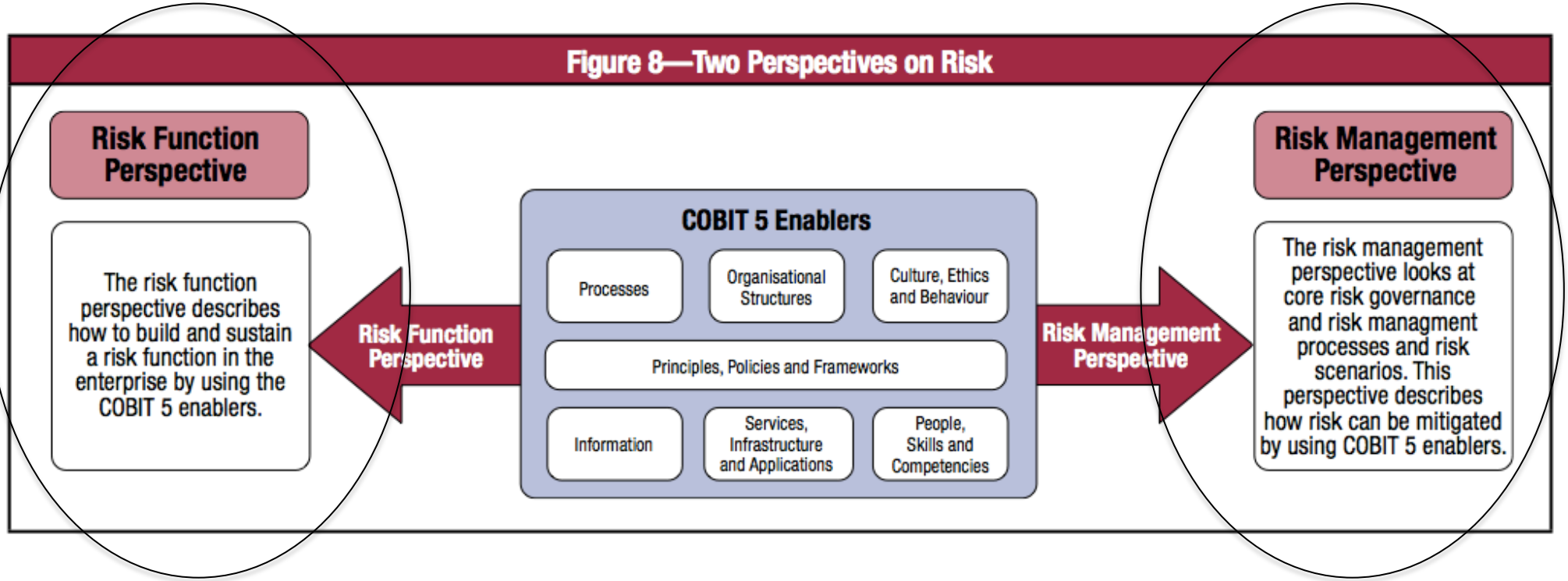
ISACA
Trust in, and value from, information systems

NEXT STEPS FOR RISK MANAGEMENT

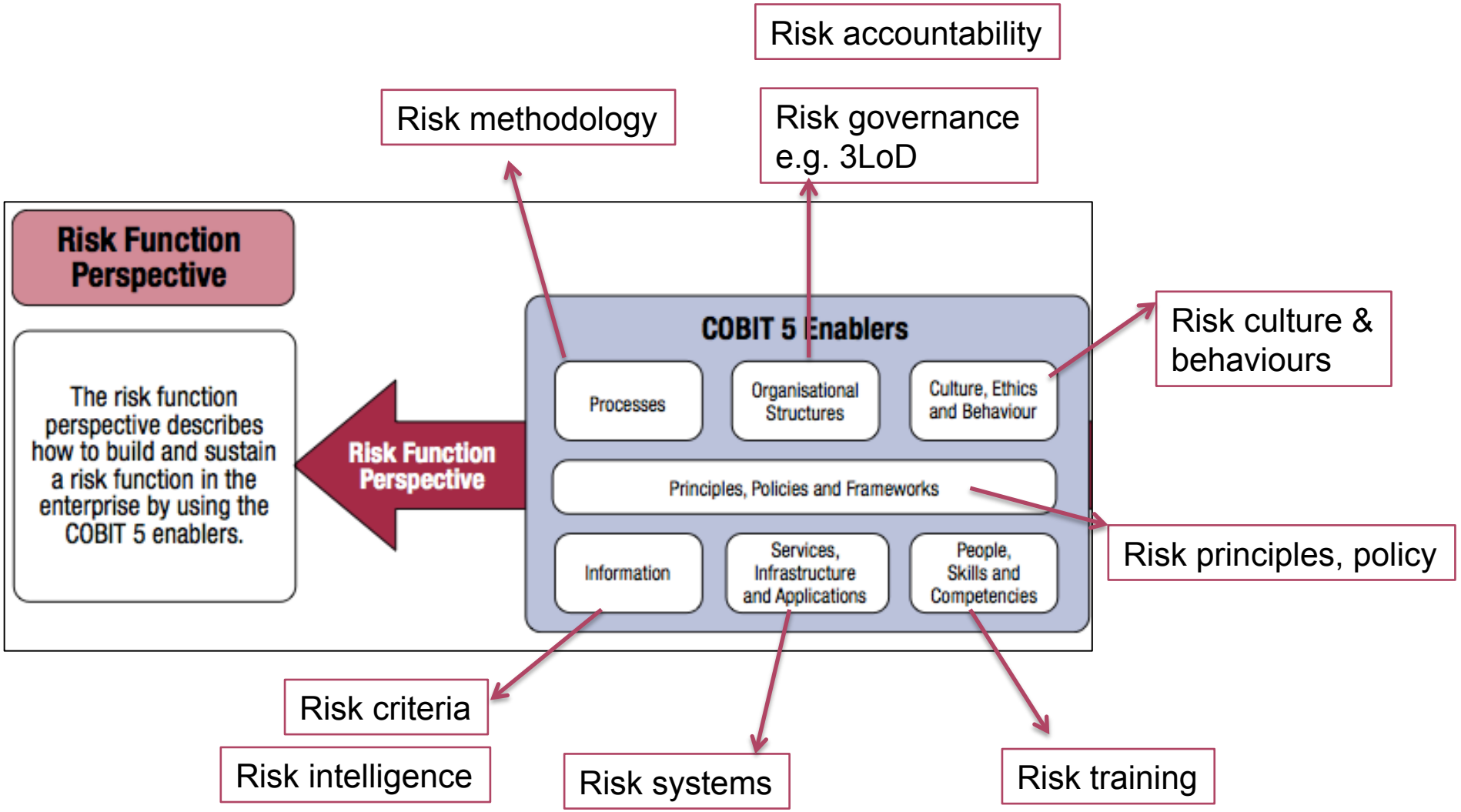
- Risk and opportunity
- **Risk capability**
- Risk scenarios
- Risk appetite

ADDRESSING TWO PERSPECTIVES ON RISK

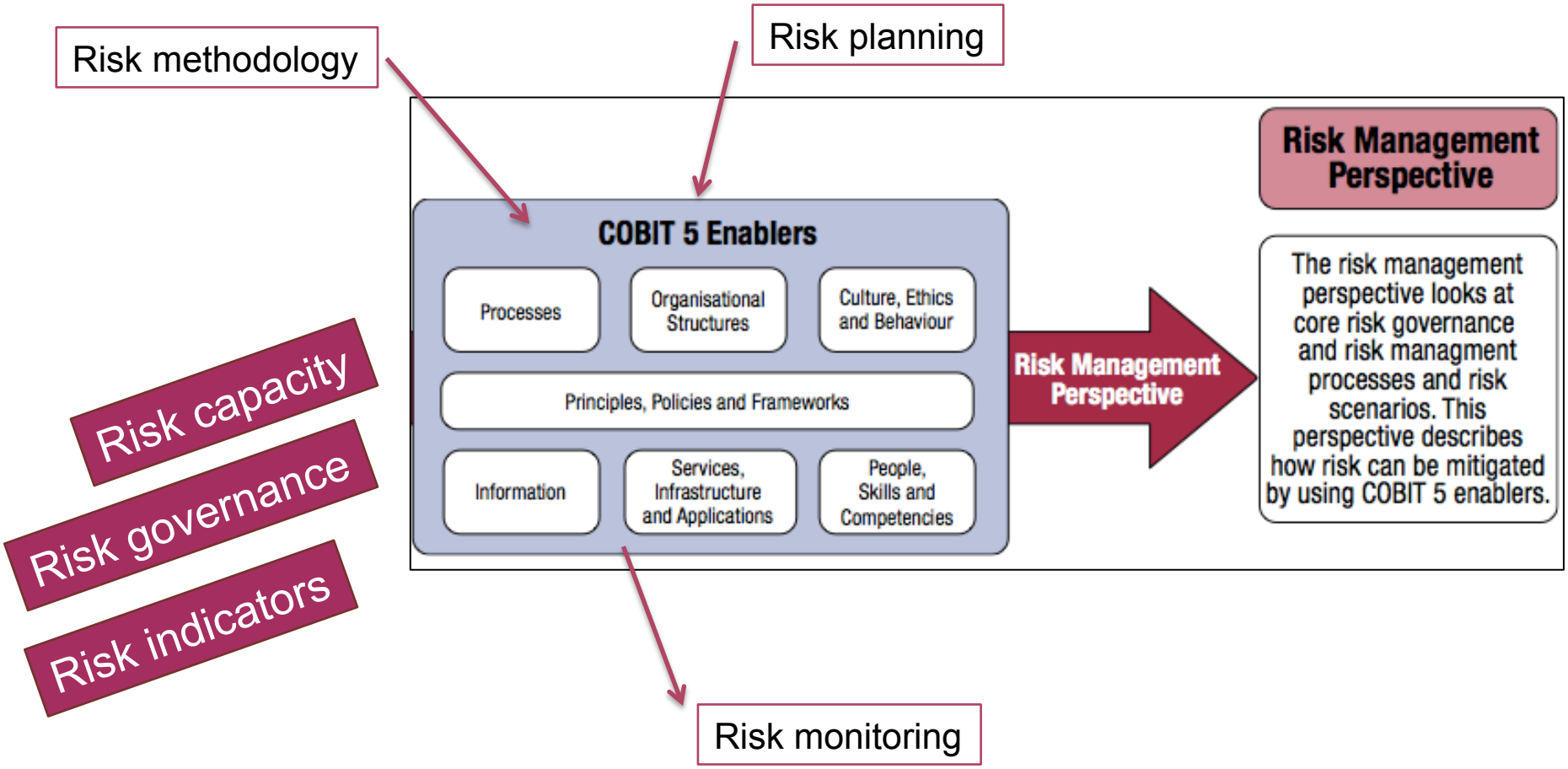




RISK FUNCTION CAPABILITIES



RISK MANAGEMENT CAPABILITIES



CORE AND SUPPORTING RISK PROCESSES

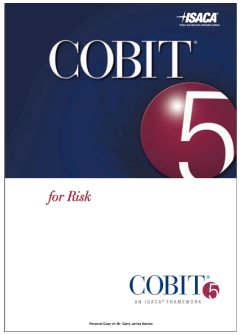


Figure 18—Supporting Processes for the Risk Function

Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

- EDM01 Ensure Governance Framework Setting and Maintenance
- EDM02 Ensure Benefits Delivery
- EDM03 Ensure Risk Optimisation
- EDM04 Ensure Resource Optimisation
- EDM05 Ensure Stakeholder Transparency

Align, Plan and Organise

- APO01 Manage the IT Management Framework
- APO02 Manage Strategy
- APO03 Manage Enterprise Architecture
- APO04 Manage Innovation
- APO05 Manage Portfolio
- APO06 Manage Budget and Costs
- APO07 Manage Human Resources
- APO08 Manage Relationships
- APO09 Manage Service Agreements
- APO10 Manage Suppliers
- APO11 Manage Quality
- APO12 Manage Risk
- APO13 Manage Security

Build, Acquire and Implement

- BAI01 Manage Programmes and Projects
- BAI02 Manage Requirements Definition
- BAI03 Manage Solutions Identification and Build
- BAI04 Manage Availability and Capacity
- BAI05 Manage Organisational Change Enablement
- BAI06 Manage Changes
- BAI07 Manage Change Acceptance and Transitioning
- BAI08 Manage Knowledge
- BAI09 Manage Assets
- BAI10 Manage Configuration

Deliver, Service and Support

- DSS01 Manage Operations
- DSS02 Manage Service Requests and Incidents
- DSS03 Manage Problems
- DSS04 Manage Continuity
- DSS05 Manage Security Services
- DSS06 Manage Business Process Controls

Monitor, Evaluate and Assess

- MEA01 Monitor, Evaluate and Assess Performance and Conformance
- MEA02 Monitor, Evaluate and Assess the System of Internal Control
- MEA03 Monitor, Evaluate and Assess Compliance With External Requirements

Processes for Management of Enterprise IT

Core risk processes

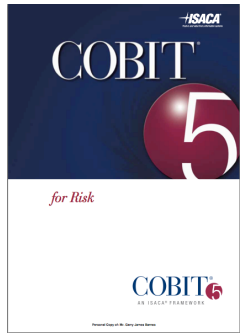
Key supporting processes

ISACA
Trust in, and value from, information systems

NEXT STEPS FOR RISK MANAGEMENT

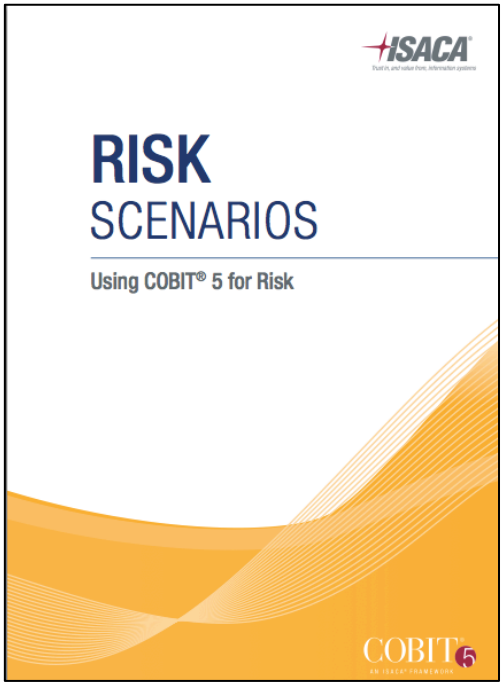
- Risk and opportunity
- Risk capability
- **Risk scenarios**
- Risk appetite

RISK SCENARIOS



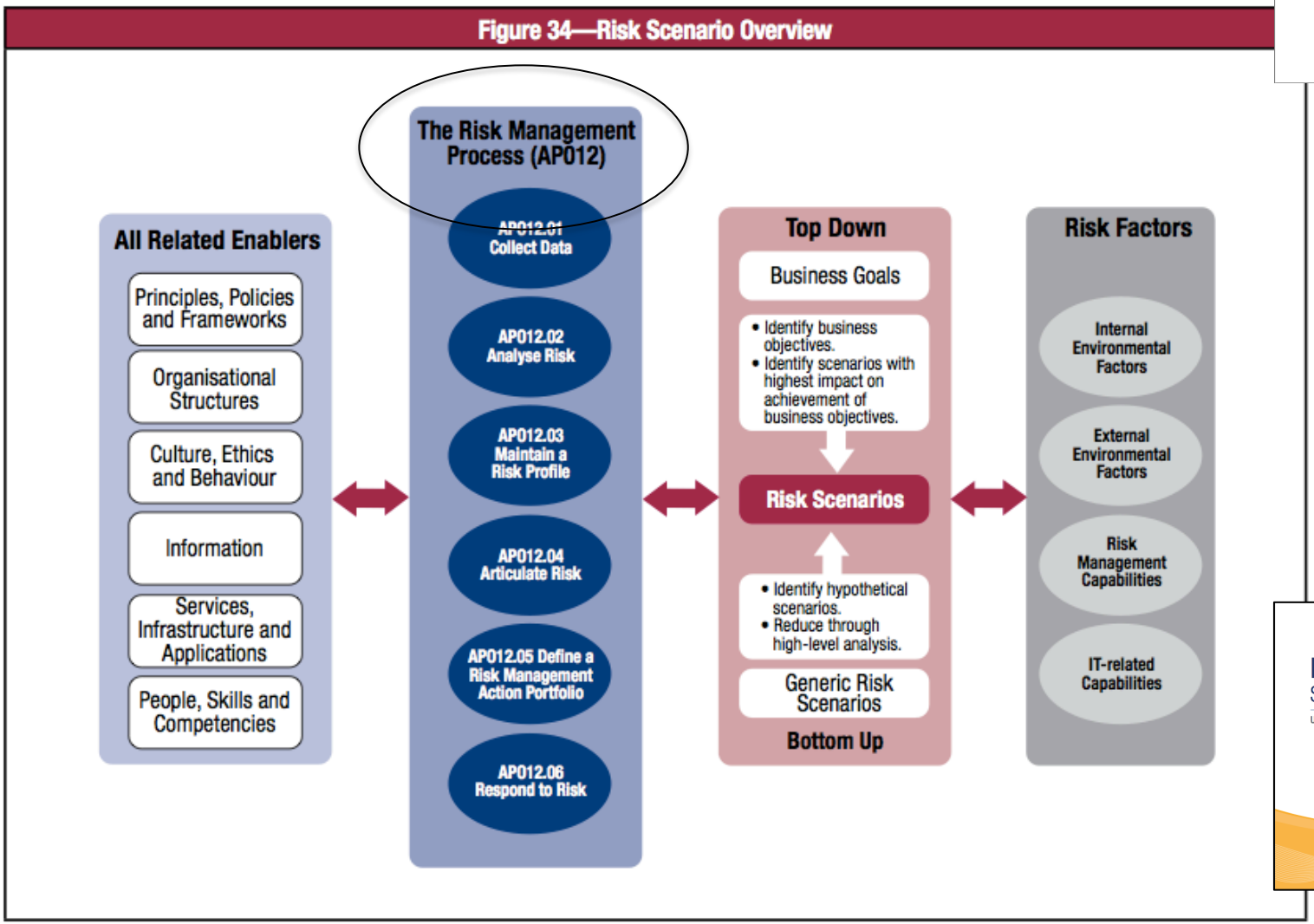
Common risk identification challenges:

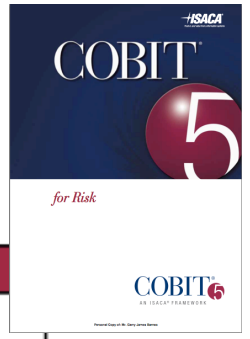
- **Volume of identifiable risks**
- **Generic risk descriptions – misalignment with business**
- **Process and control failure risks – incidents!**
- **Over specification of risk detail**
- **Repetition of risk across BU's**

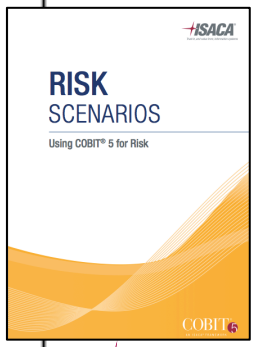


ISACA®
Trust in, and value from, information systems

RISK SCENARIOS







ISACA®
Trust in, and value from, information systems

NEXT STEPS FOR RISK MANAGEMENT

- Risk and opportunity
- Risk capability
- Risk scenarios
- **Risk appetite**

WHAT IS RISK APPETITE?

ISO 31000:

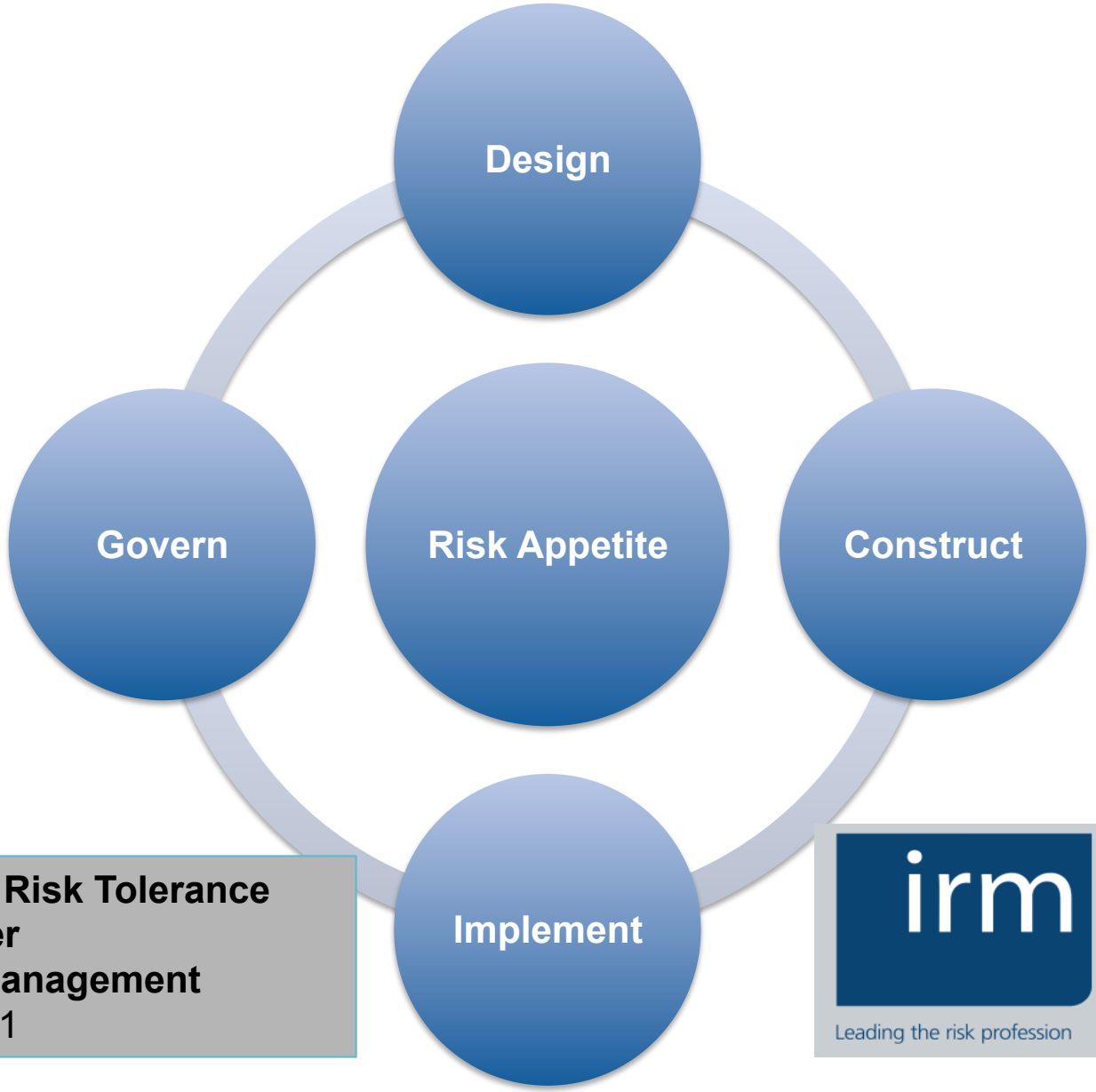
Amount and type of risk that an organisation is willing to pursue or retain

COBIT 5 for Risk

The broad-based amount of risk … that an enterprise is willing to accept in pursuit of its mission (or vision).

“Acceptable Level of Risk”

DESIGNING RISK APPETITE



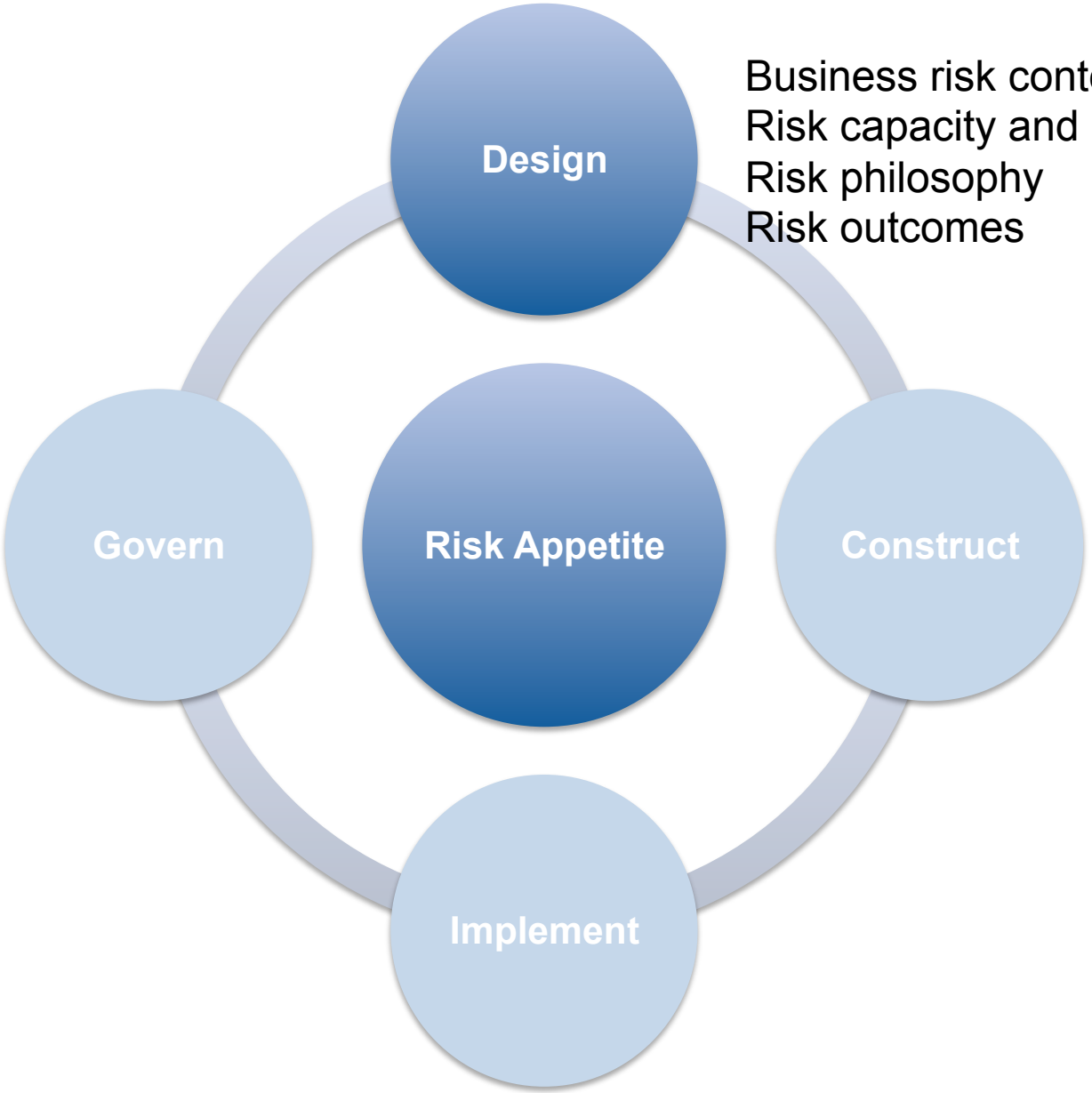
Risk Appetite and Risk Tolerance
Consultation paper
Institute of Risk Management
May 2011 – Figure 1

Used with permission

irm
Leading the risk profession

ISACA
Trust in, and value from, information systems

DESIGNING RISK APPETITE



Business risk context
Risk capacity and capability
Risk philosophy
Risk outcomes

ISACA
Trust in, and value from, information systems

POOR POLICIES INHIBIT OPTIMISING RISK

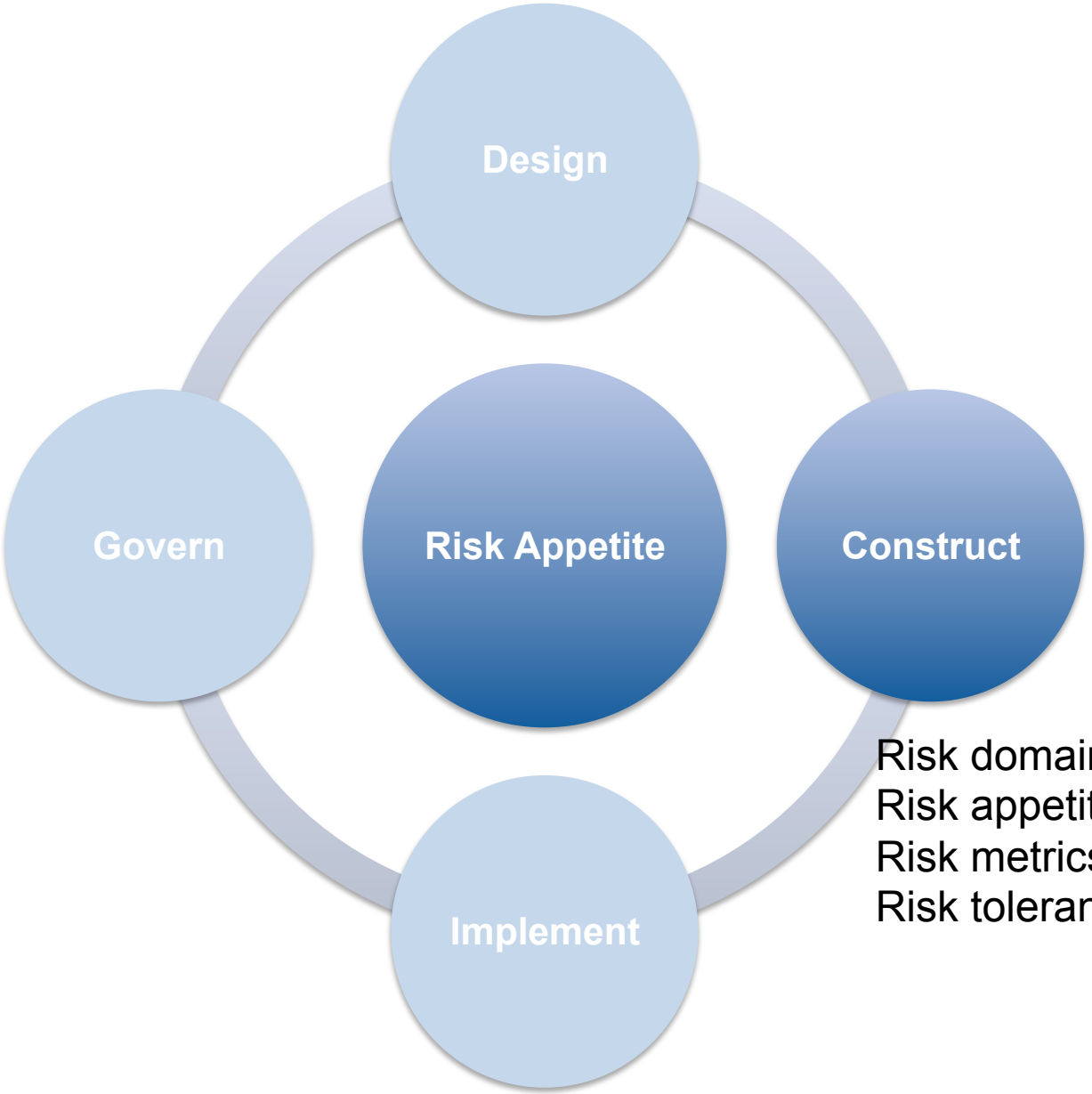
Policy often preceded Risk Appetite Statements:

- Legacy effect of historic policy positions
- Enterprise-wide policies lack granularity for local risk/reward decisions
- Tightening of policies after incidents

Codes of Conduct:

- Great place to start when developing a Risk Appetite Statement
- Language the Board and Executives understand
- Often covers some key areas of risk – expectations, compliance

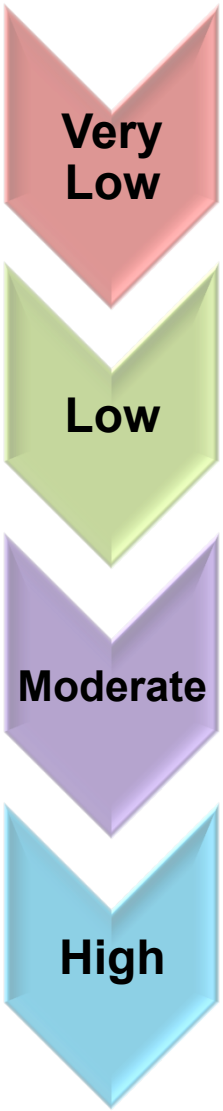
CONSTRUCTING RISK APPETITE



Risk domains
Risk appetite statements
Risk metrics (KRIs)
Risk tolerances

ISACA
Trust in, and value from, information systems

DETAILED RISK APPETITE STATEMENTS



- Avoid exposures
- Ensure awareness and operation of controls
- Assurance of KPIs and KRIs

e.g. compliance risk

- Minimise risk exposures
- Provide awareness and operation of controls
- Monitor and report KPIs and KRIs

e.g. operational risk

- Allow local decisions for risk/reward, cost/benefit
- Use timely risk information to drive risk response

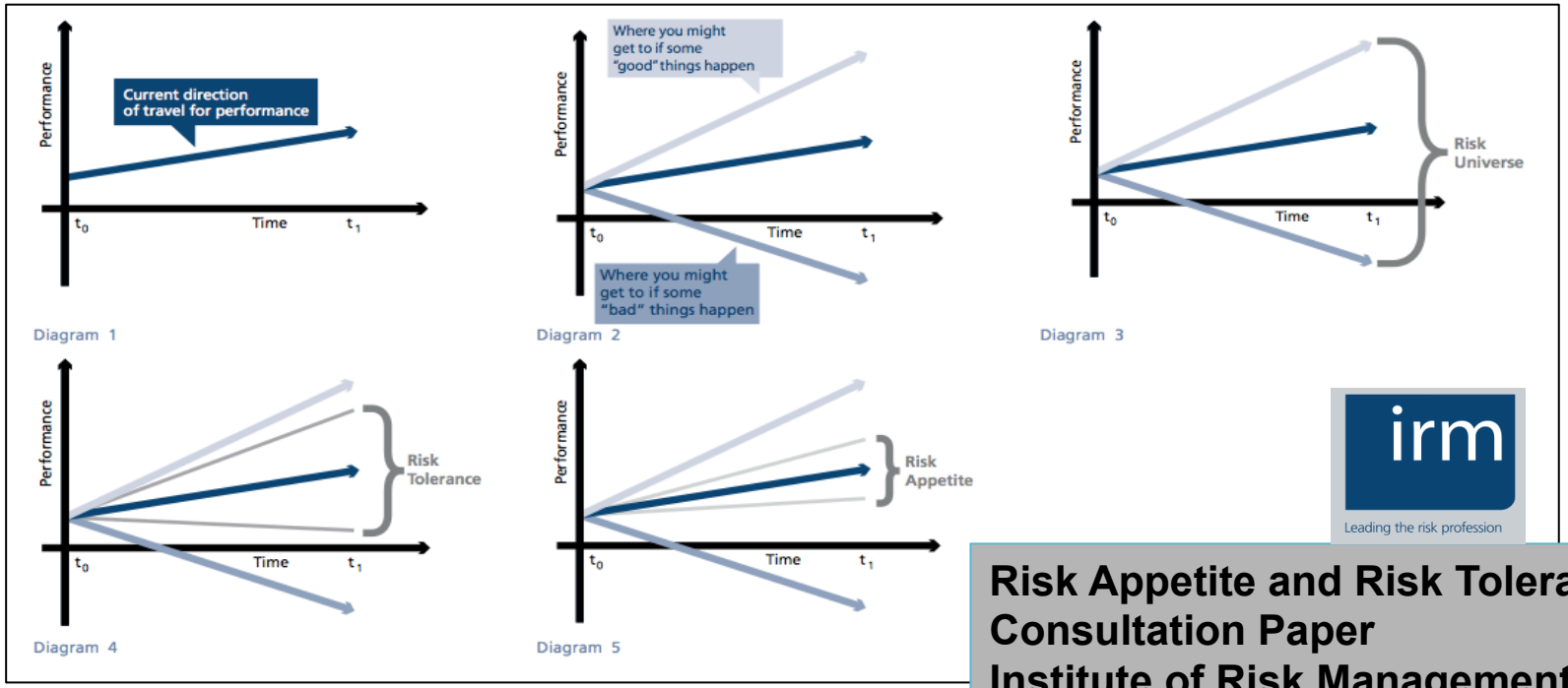
e.g. program risk

- Seek strategic opportunities
- Manage risk and return
- Communicate expectations and outcomes

e.g. investment risk

RISK TOLERANCE

Risk tolerance levels are tolerable deviations from the level set by the risk appetite definitions

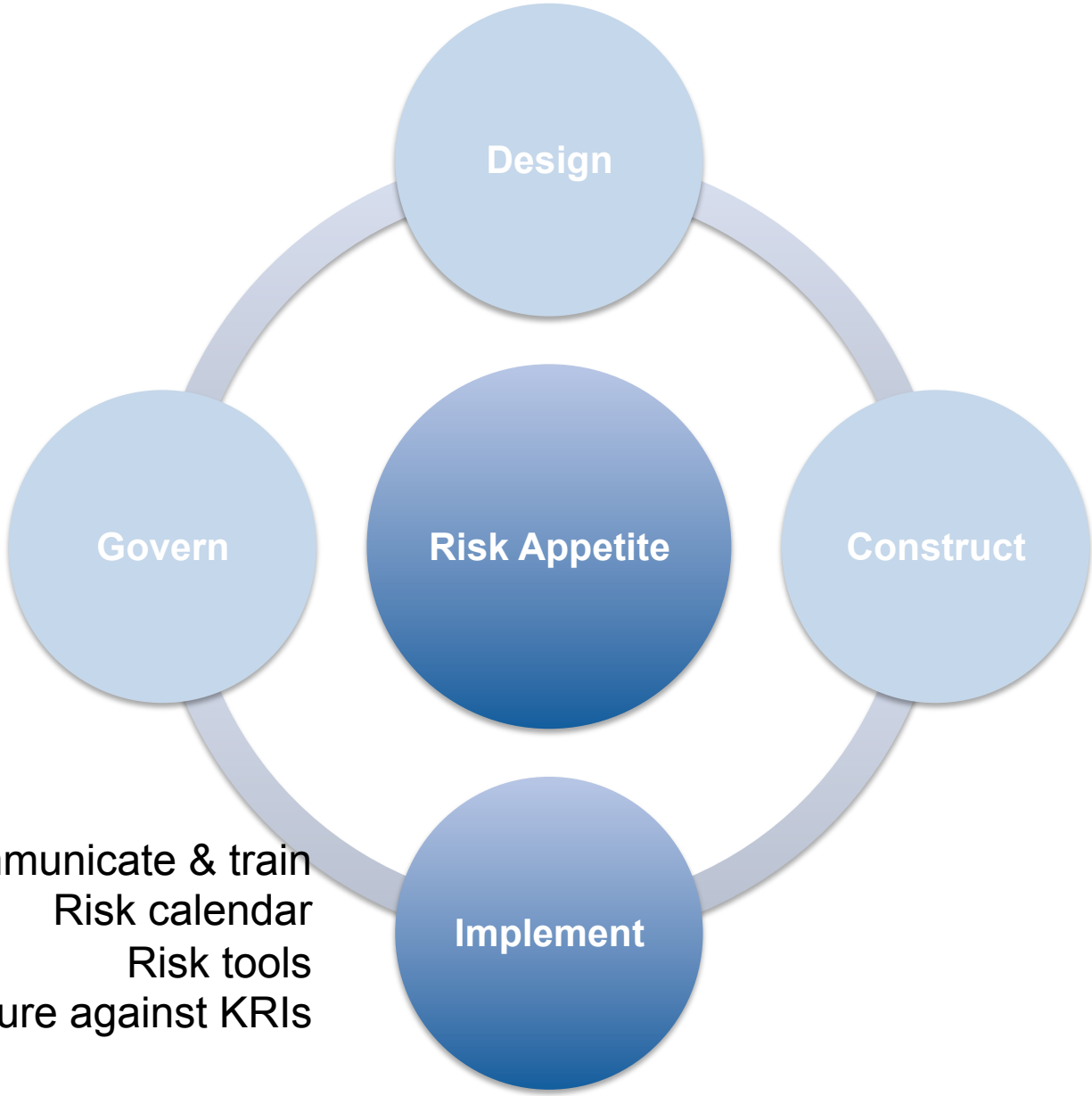


Risk Appetite and Risk Tolerance Consultation Paper
Institute of Risk Management
2011

Used with permission

ISACA
Trust in, and value from, information systems

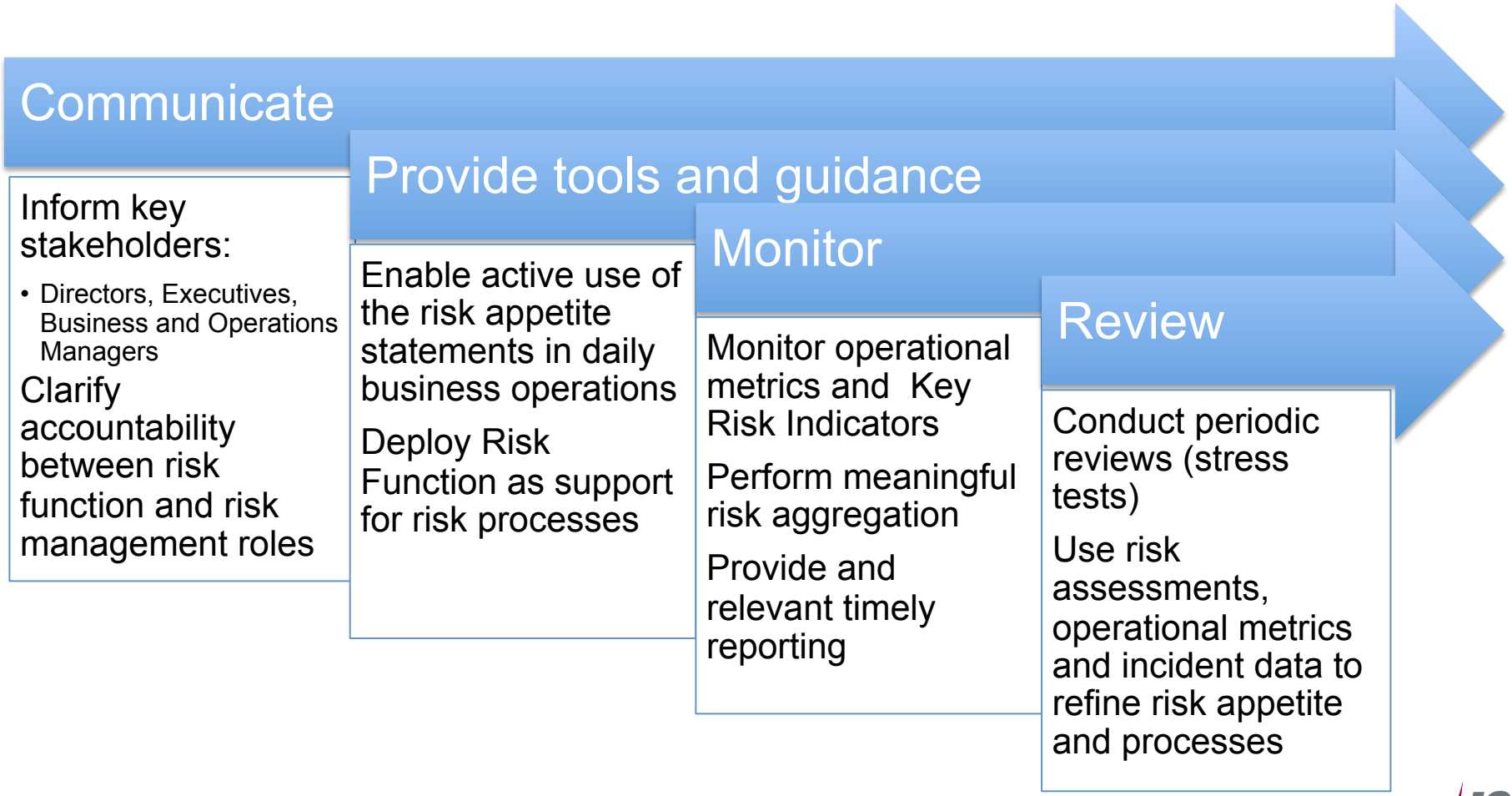
IMPLEMENTING RISK APPETITE



Communicate & train
Risk calendar
Risk tools
Measure against KRIs

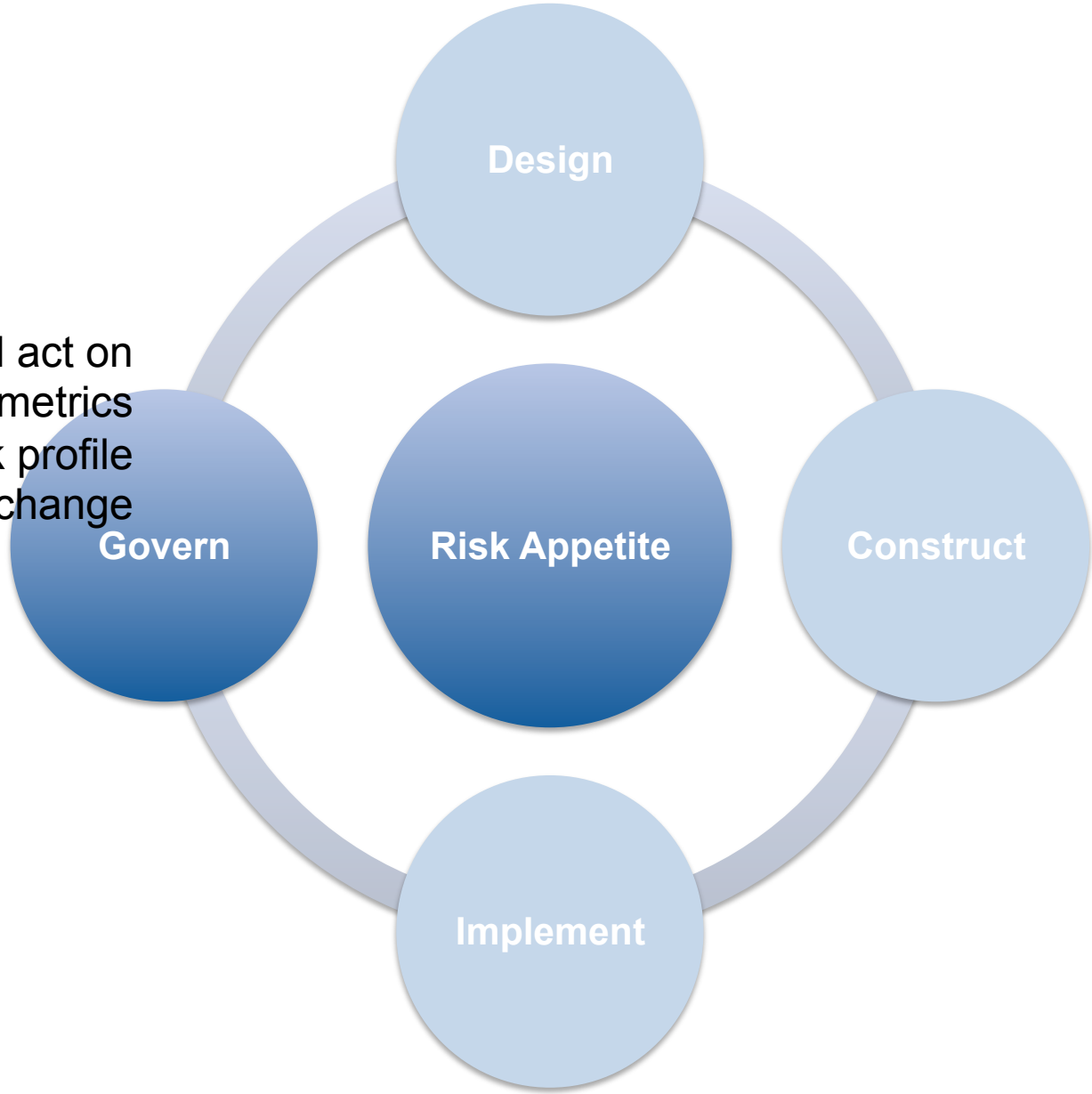
ISACA
Trust in, and value from, information systems

IMPLEMENTING RISK APPETITE



GOVERNING RISK APPETITE

Assess and act on metrics
Monitor risk profile
Monitor business change



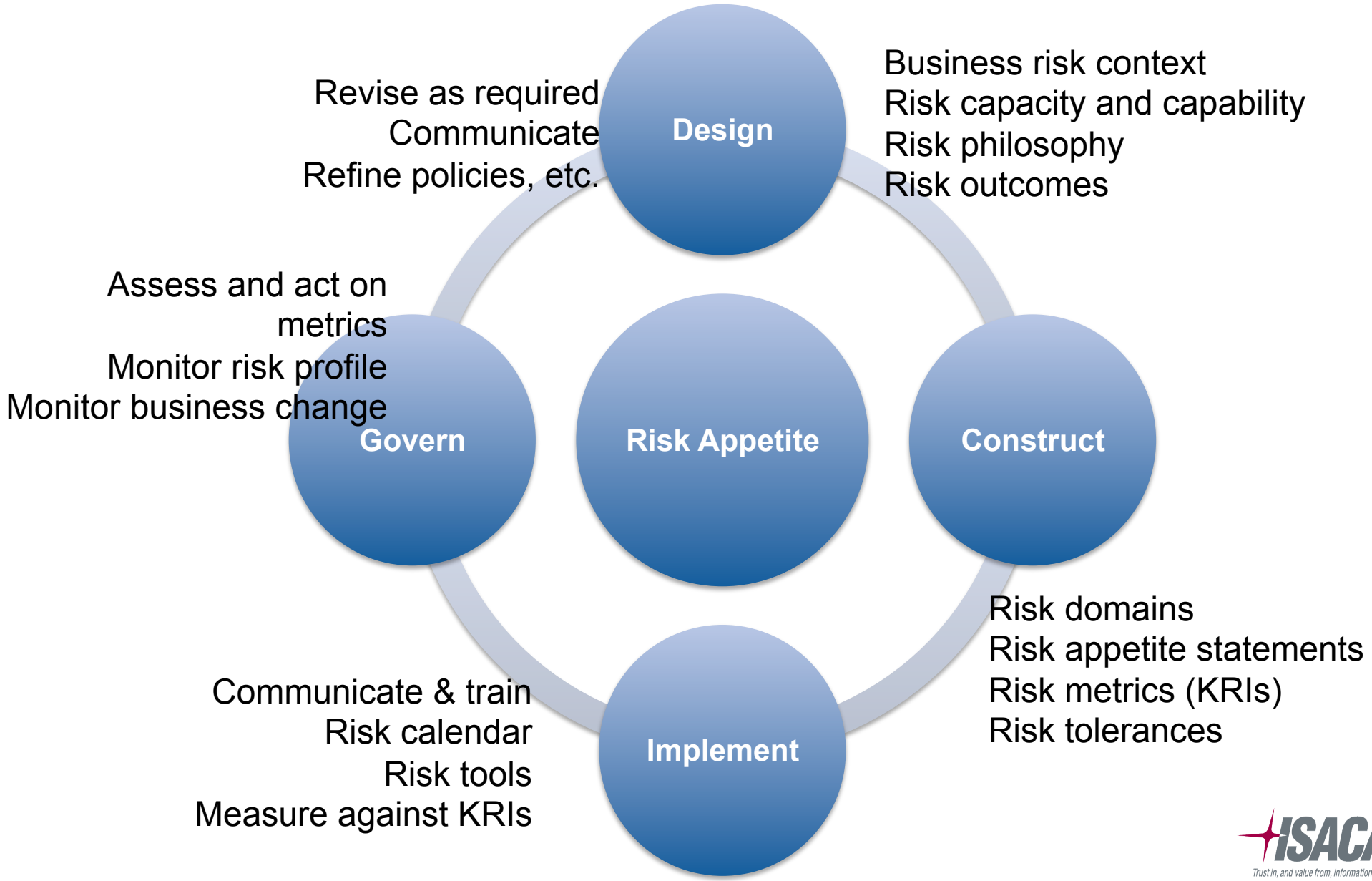
ISACA
Trust in, and value from, information systems

RE-DESIGNING RISK APPETITE

Revise as required
Communicate
Refine policies, etc.

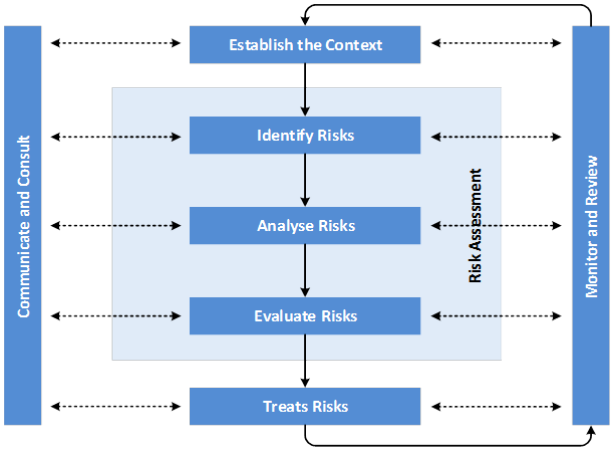
ISACA
Trust in, and value from, information systems

SUMMARY: DESIGNING RISK APPETITE



ISACA
Trust in, and value from, information systems

EXPLORING THE CHALLENGES – OBTAINING VALUE



Risk and opportunity

Risk capability

Risk scenarios

Risk appetite

“The best risk management is about managing risk to business performance against specific outcomes or objectives.”

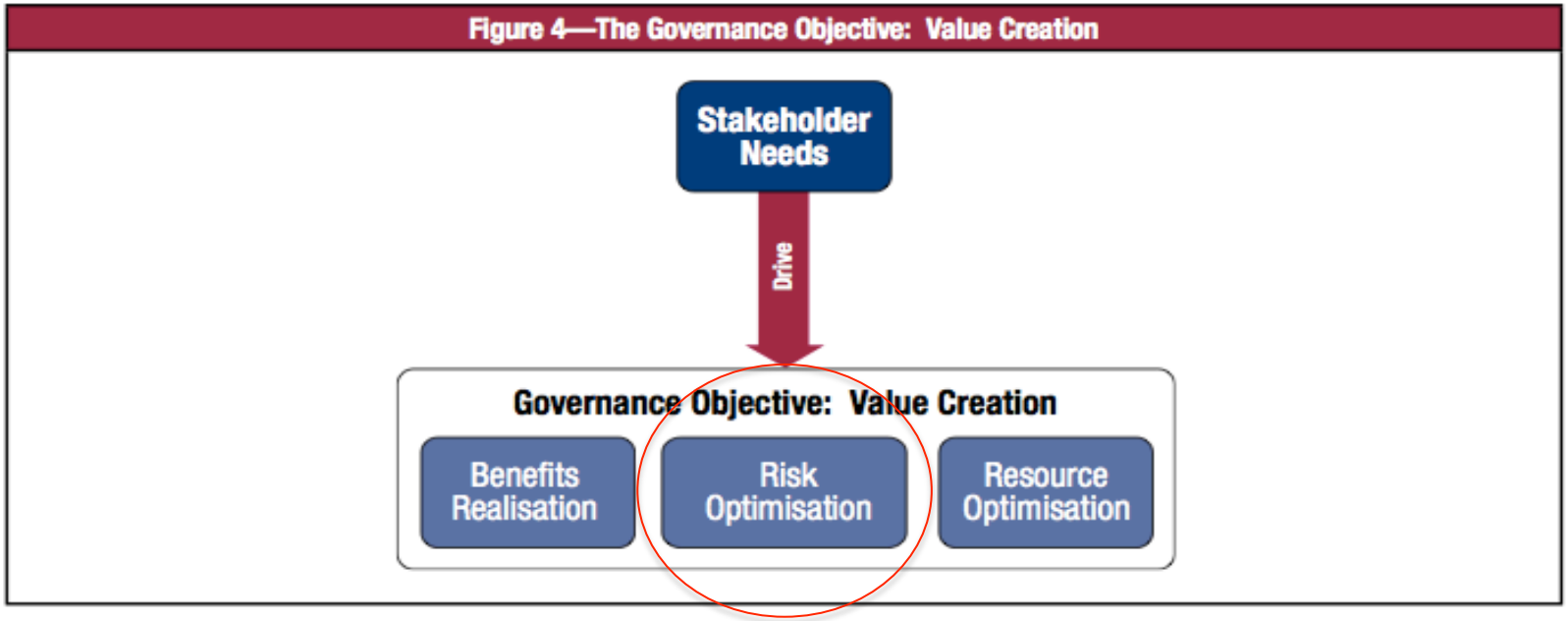
Excerpt From: Brian Barnier “The Operational Risk Handbook for Financial Companies: A guide to the new world of performance-oriented operational risk.”

COBIT 5 – "RISK OPTIMISATION"

COBIT 5
AN ISACA® FRAMEWORK

The Governance Objective:

"Value creation means realising benefits at an optimal resource cost while optimising risk"



ISACA®
Trust in, and value from, information systems

QUESTIONS?

ISACA®
Trust in, and value from, information systems