# ISACA's Risk IT in a Cloud-based environment

**Kamal Khan, CISA, CISSP, MBCS, CITP**
**Director, ISACA London Chapter**

March 2020

ISACA®
London Chapter

# Agenda

- Introduction
- Risk IT
- Using Risk IT in a Cloud Environment
- Conclusion

# Introduction

- Kamal Khan, Director of ISACA London Chapter
- Over 30 years experience in Information Systems Audit and Control
- Worked in Banking, Utilities, Oil and Gas industries
- Worked on initial version of Risk IT and current one which is being revised as Subject Matter Expert
- ISACA London Chapter:
- ISACA® is the voice of the information systems audit, IT governance, risk management and cybersecurity professions.
- The ISACA London Chapter
  - First in the UK
  - Established in 1981
  - Over 4,200 members, largest in the world

ISACA®
London Chapter

# Risk IT

# Who uses a formal risk management process for their Cloud environment?

ISACA

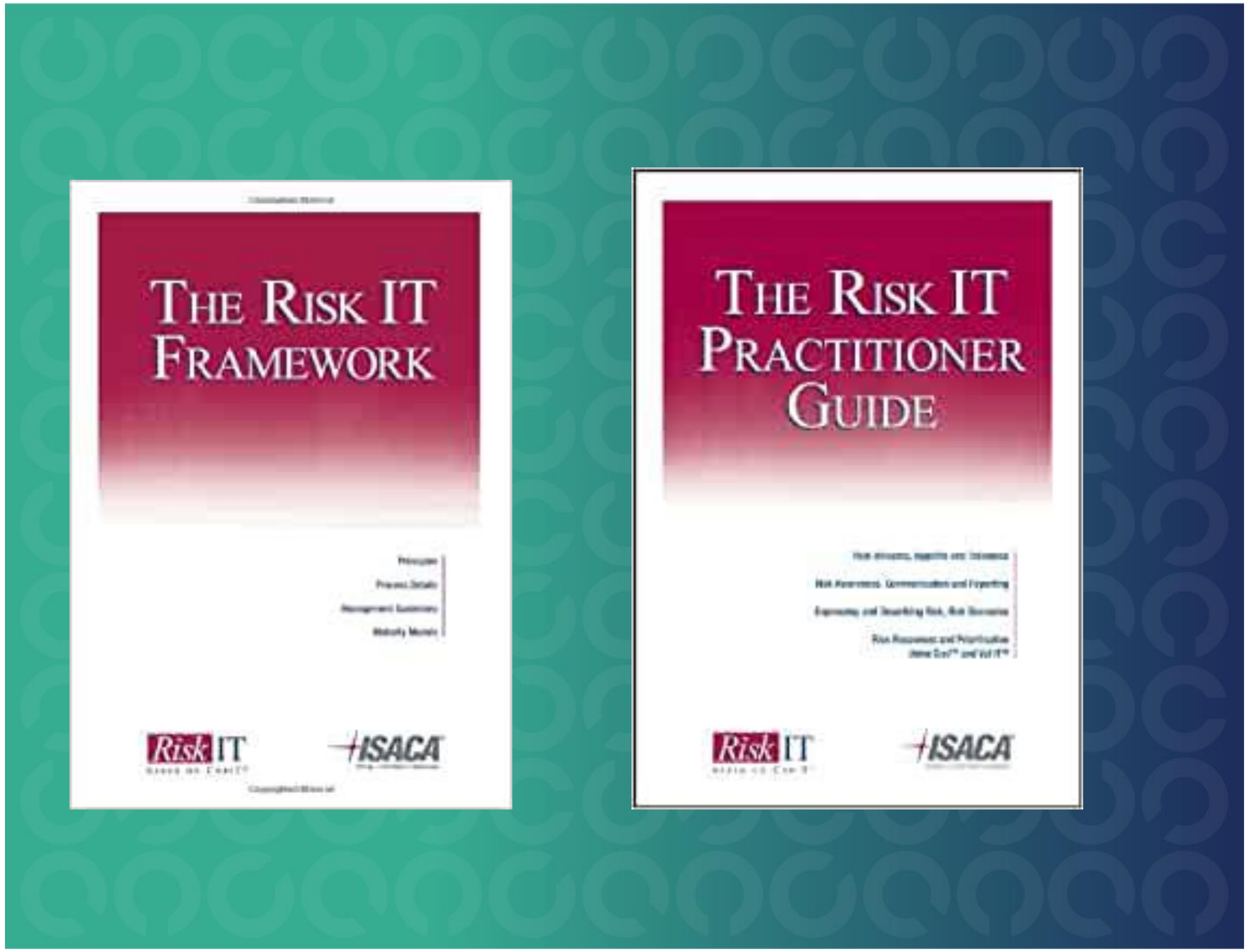
London Chapter

# Who has heard of ISACA Risk IT?

ISACA London Chapter

# What is Risk IT

- An ISACA publication.
- An end-to-end, comprehensive view of all risks related to the use of IT
- Consists of two documents
  - The Risk IT Framework
  - The Risk IT Practiotoner Guide



The Risk IT Framework

Risk IT

ISACA

The Risk IT Practitioner Guide

Risk IT

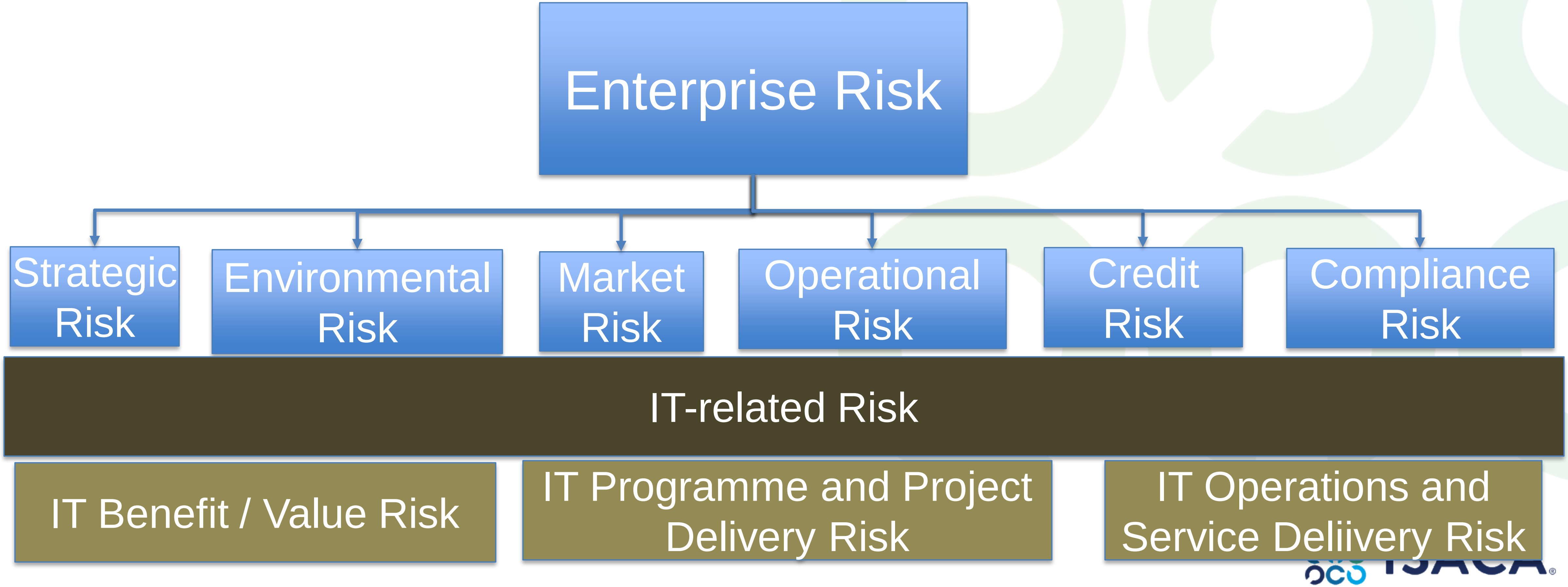
ISACA

# Risk IT Principles

# Can we treat Risks in IT separately Enterprise Risk?

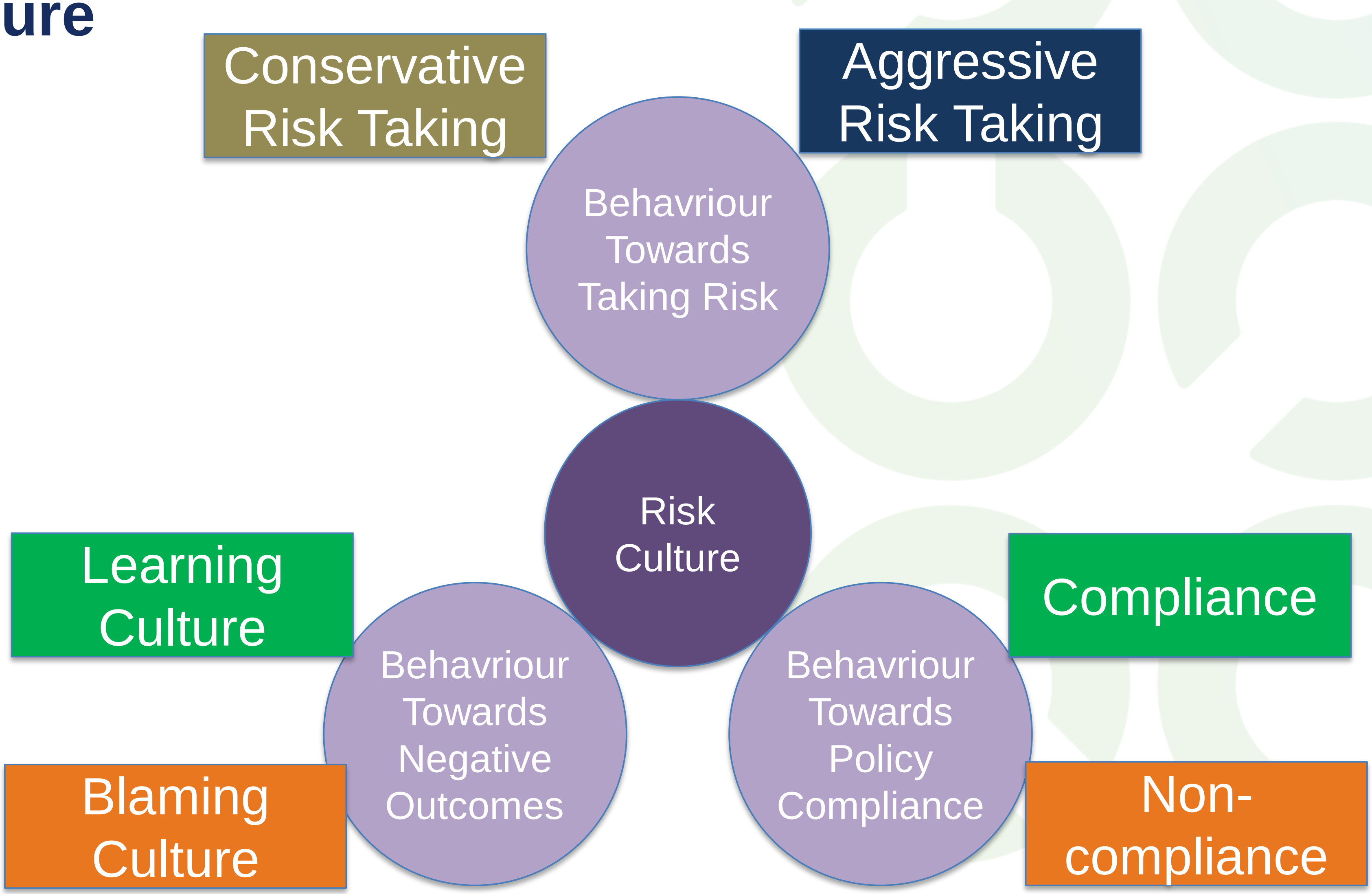
# Risk Universe

- IT Risk is a component of the overall risk universe
- Also a component of Strategic Risk, Environmental risk etc



London Chapter

# Risk Culture



Conservative Risk Taking

Aggressive Risk Taking

Behavriour Towards Taking Risk

Risk Culture

Learning Culture

Blaming Culture

Behavriour Towards Negative Outcomes

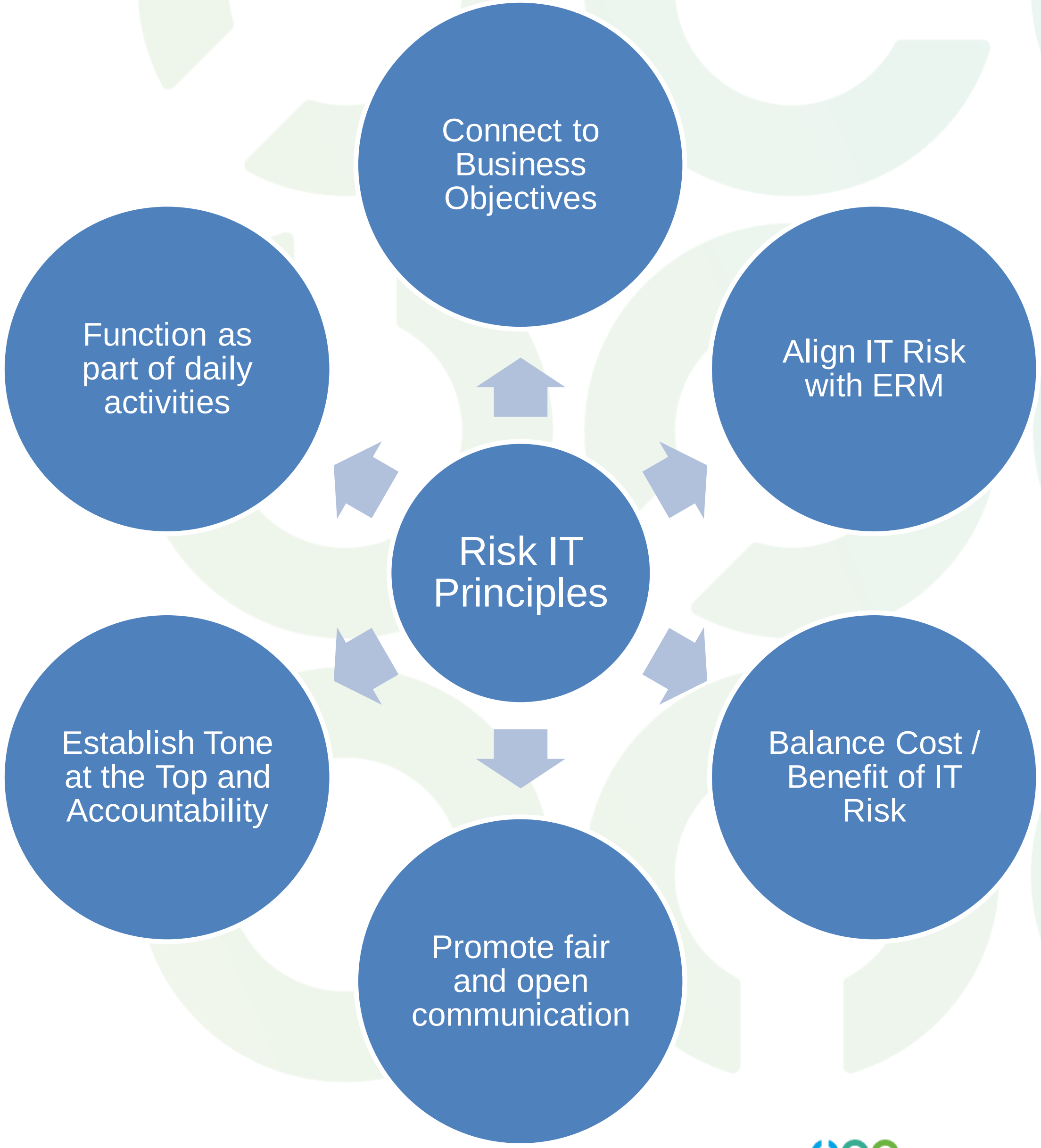
Behavriour Towards Policy Compliance

Compliance

Non-compliance

# Risk IT Principles

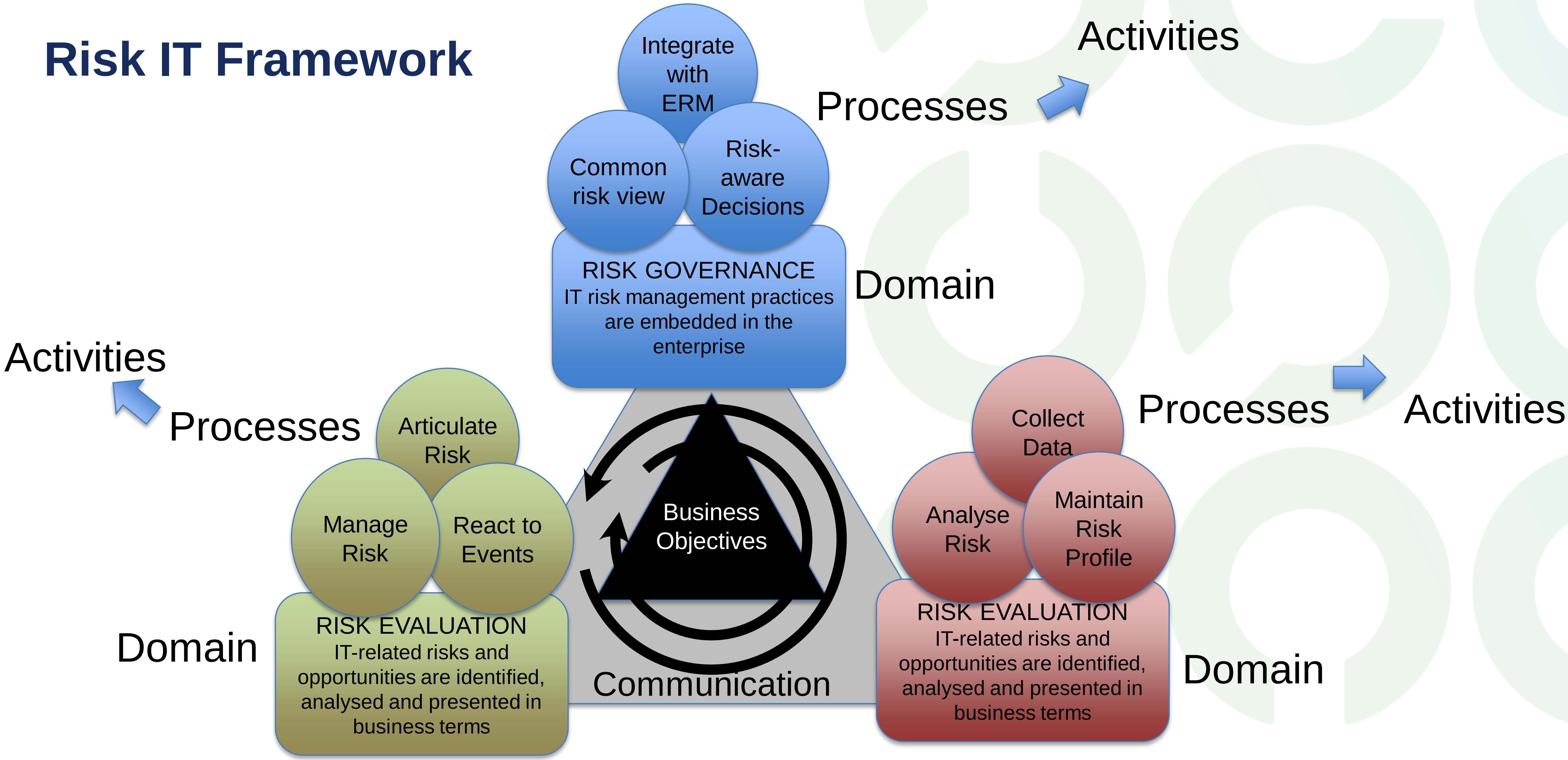
- Risk IT is about business risk related to the use of IT:
- Always connect to business objectives
- Align the management of IT-related business risk with overall ERM
- Balance the costs and benefits of managing IT risk
- Establish the right tone from the top and define and enforce personal accountability for operating within tolerance levels
- A continuous process and part of daily activities


Connect to Business Objectives
Align IT Risk with ERM
Balance Cost / Benefit of IT Risk
Promote fair and open communication
Establish Tone at the Top and Accountability
Function as part of daily activities
Risk IT Principles

ISACA London Chapter

# Risk IT Framework

# Risk IT Framework



# Risk Governance

# Common Risk View

Defining a Risk Universe

- Objective:
  - Define and describe the overall environment subject to risk management

- Define:
  - The Entity
  - External Environment
  - Internal Environment
  - Risk Management Capability
  - IT Management Capability

- Considerations in a Cloud environment:
  - Ceding control to the Cloud Provider (CP)
  - Impact on the organization’s strategy and capacity to meet its mission and goals
  - Impossibility of complying with the security requirements
  - Deterioration of performance and quality of service
  - Introduction of compliance challenges.

ISACA London Chapter

# Risk Evaluation

# Analyse Risk

## Estimate IT Risk

- Objective:
- Define and understand IT-related risk using risk scenario analysis.
- Risk scenario analysis is a technique to make IT risk more concrete and tangible

- IT Risk Scenarios:
- Actor or
- Threat type
- Event
- Asset / Resource
- Time: Timing, Duration, Time lag

- Cloud environment risk example scenario:
- Actor: External attacker
- Threat Type: Malicious act
- Event: Disclosure
- Asset: Encryption Keys
- Time: Immediate downtime / Data may not be recoverable / Immediately detected

ISACA London Chapter

| High Level Risk Scenario | Actor | Threat Type | Event | Asset / Resource | Time | Negative Example Scenarios | Positive Example Scenarios |
|---|---|---|---|---|---|---|---|
| Selection / Performance of Cloud provider | Internal | Failure | Ineffective design | Ineffective design | ◉Timing (non-critical)<br>◉ Duration (extended)<br>◉ Detecion (slow) | ◉ Inadequate support and services from Cloud Provider<br>◉ Inadequate performance of Cloude Provider | Cloud Provier as a strategic partner |
| Cloud expertise and skills | Internal | Failure | Ineffective design | Process (manage IT human resources) | ◉Timing (unknown)<br>◉ Duration (extended)<br>◉ Detecion (instant) | ◉ Lack or mismatch of Cloud-related skills | ◉Attracting the appropriate staff increases service delivery<br>◉ Correct staff and skill mix will support project delivery and value delivery |
| Contractual Compliance | ◉ External | Failure | ◉ Ineffective execution | ◉ Process (ensure compliance to external requirements) | ◉Timing (non-critical)<br>◉ Duration (extended)<br>◉ Detecion (slow) | ◉ Contractual obligations with customers not met | |
| Logical Tresassing | ◉ Internal<br>◉ External | Malicious | ◉ Ineffective design<br>◉ Inappropriate use<br>◉ Disclosure | ◉ Process (ensure systems security)<br>◉ Enterprise architecture (information) | ◉Timing (non-critical)<br>◉ Duration (extended)<br>◉ Detecion (slow) | ◉Users circumventing logical acces rights<br>◉ Users obtaining access to unauthorised information<br>◉ Users stealing sensitive data | |
| Data protection risks | ◉ Internal<br>◉ External | Disclosure | Personal sensitive data | ◉ Process (ensure systems security)<br>◉ Enterprise architecture (information) | ◉Timing (non-critical)<br>◉ Duration (extended)<br>◉ Detecion (slow) | ◉Users circumventing logical acces rights<br>◉ Users obtaining access to unauthorised information<br>◉ Users stealing sensitive data | |

| High Level Risk Scenario | Actor | Threat Type | Event | Asset / Resource | Time | Negative Example Scenarios | Positive Example Scenarios |
|---|---|---|---|---|---|---|---|
| Selection / Performance of Cloud provider | Internal | Failure | Ineffective design | Ineffective design | ◉Timing (non-critical)<br>◉ Duration (extended)<br>◉ Detecion (slow) | ◉ Inadequate support and services from Cloud Provider<br>◉ Inadequate performance of Cloude Provider | Cloud Provier as a strategic partner |

ISACA®
London Chapter

# Manage risk

# Manage Risk

Implement controls

- Objective:
- Provide guidance on how CobiT control objectives and management practices can help in risk mitigation activities.

- Generic Scenarios:
- Control Title
- Control Description

- Cloud environment risk example scenario:
- Generic scenario: Cloud provider Selection
- Control Title: Supplier Selection
- CobiT Control Objective: Select Cloud provider according to a fair and formal practice

| Generic Scenario | Control Title | CobiT Control Objective |
|---|---|---|
| Cloud provider Selection | Supplier Selection | Select Cloud provider according to a fair and formal practice to ensur a viable best fit based on specified requirements. Requirements should be optimised with input from potential suppliers |
| | Supplier Relation Management | Formalise the relationship management processs for each Cloud provider. Ensure the quality of the relationship based on trust and transparency (eg through SLA's) |
| Contractual Compliance | Supplier Contract Management | Set up a proceudre for establishing, modifyng and terminating contracts for Cloud provders. Include minimum, legal, financial, etc responsibilities and liabilities |
| IT expertise and skills | Personnel recruitment and retention | Maintain it personnel recruitment processes to ensure that the organsation has an adequate Cloud expertise |
| | Personnel Training | Provide employees with on-going training to maintain their Cloud knowledge and skills. |
| Logical Tresassing | Security Testing, Surveillance and monitoring | Test and monitor the IT security to ensure that the information security baseline is maintained. A logging and monitoring function will enable early prevention and / or detectionof unusual activities |
| Data protection risks | Security Requirements for Data Management | Define and implement policies and procedures to identify and apply security requirements appicable to the receipt, processing, storage and output of data |

| Generic Scenario | Control Title | CobiT Control Objective |
|---|---|---|
| Cloud provider Selection | Supplier Selection | Select Cloud provider according to a fair and formal practice to ensur a viable best fit based on specified requirements.  Requirements should be optimised with input from potential suppliers |
| | Supplier Relation Management | Formalise the relationship management processs for each Cloud provider.  Ensure the quality of the relationship based on trust and transparency (eg through SLA's) |

# Conclusion

- Risk IT is a a powerful tool that can help manage all aspects of Cloud environment
- Provides all the tools you need to manage wrapped into a practical and comprehensive framework.
- Has a strong business focus that enables the Board, Management, Regulators, Service Providers, IT Departments and Users to speak a common language.

ISACA®

London Chapter