Redefining & Strengthening IT Governance through Three Lines of Defense

Presented by
Ronke Oyemade, CISA, CRISC, PMP
CEO, Principal Consultant,
Strategic Global Consulting L.L.C

Introduction

- **Brief Introduction of the Presenter.**

- **Session Presentation: 'Redefining & Strengthening IT Governance through Three Lines of Defense"**

  This session takes a different and practical approach to strengthening IT Governance by applying the three lines of defense model. This approach adopts the use of Risk IT and Cobit as frameworks through which the three lines of defense model is implemented. The session gives an overview of the three lines of defense model, Risk IT and Cobit frameworks and provides practical application of them to the IT environment of a fictitious enterprise.

- **Benefits obtained from this session.**

Agenda

1. Use of IT and IT Risk
2. IT Governance: Overview and Importance
3. Overview of Three Lines of Defense, Risk IT and Cobit Framework
4. Three Lines of Defense Model
5. What is the relationship between Risk IT Framework and Cobit Framework
6. How do the Risk IT Framework and Cobit fit into the Three Lines of Defense Model
7. First Line of Defense
8. Second Line of Defense
9. Three Line of Defense

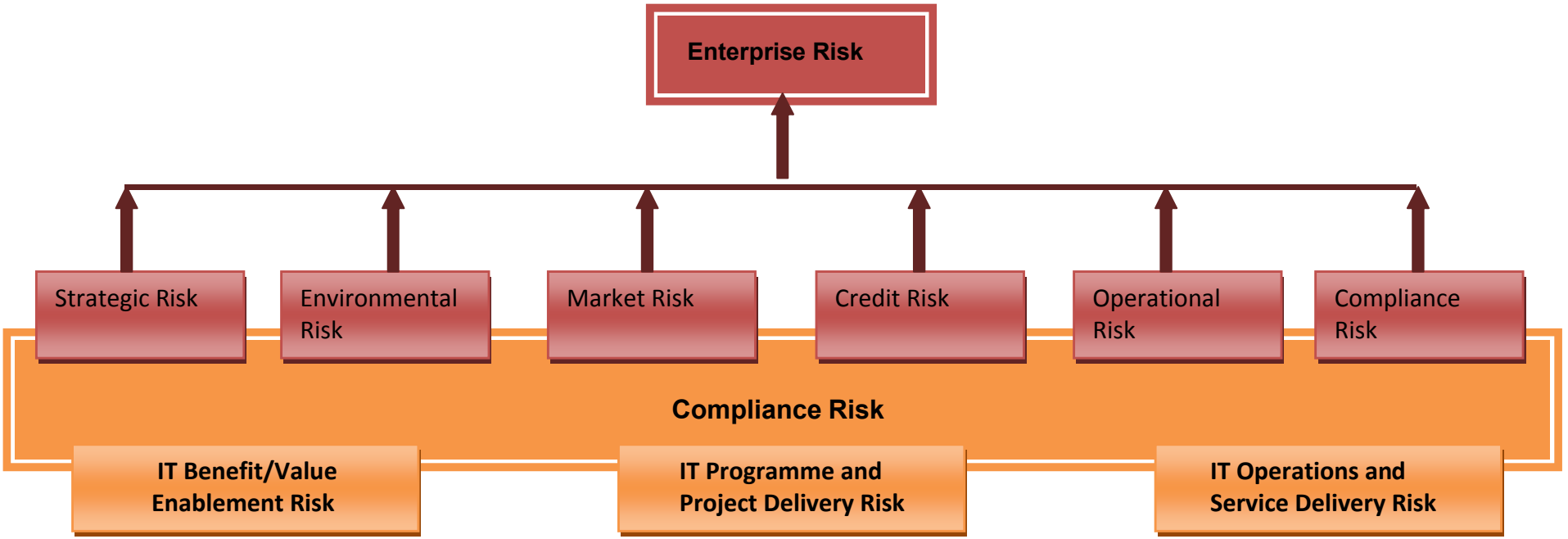
Use of IT and IT risk

- What is the importance of IT?
- Why is IT Risk?

What is IT risk?

- IT risk is business risk and a component of overall risk universe of the enterprise.
- IT-related risk is a component of other business risks

IT risk as Business Risk



Types of IT risks

	Examples
IT Benefit/ Value Enablement	•Technology enabler for new business initiatives •Technology enabler for efficient operations
IT Programme and Project Delivery	•Project quality •Project Relevance •Project Overrun
IT Programme and Project Delivery	•Project quality •Project Relevance •Project Overrun

IT Governance: Overview and Importance

- Current economic crisis & governance
- What is IT governance ?
- Why is IT governance important?

Overview of Three Lines of Defense, Risk IT and Cobit Framework

- High-level overview of Three Lines of Defense, Risk IT and Cobit Framework

Three Lines of Defense Model

First Line of Defense

Responsibility: Business operations performs day-to-day risk management activity

Function: An established risk and control environment

Second Line of Defense

Responsibility: Oversight functions such as finance, HR, Quality, and Risk Management, define policy and provide assurance.

Function: Strategic management, policy and procedure setting, functional oversight

Third Line of Defense

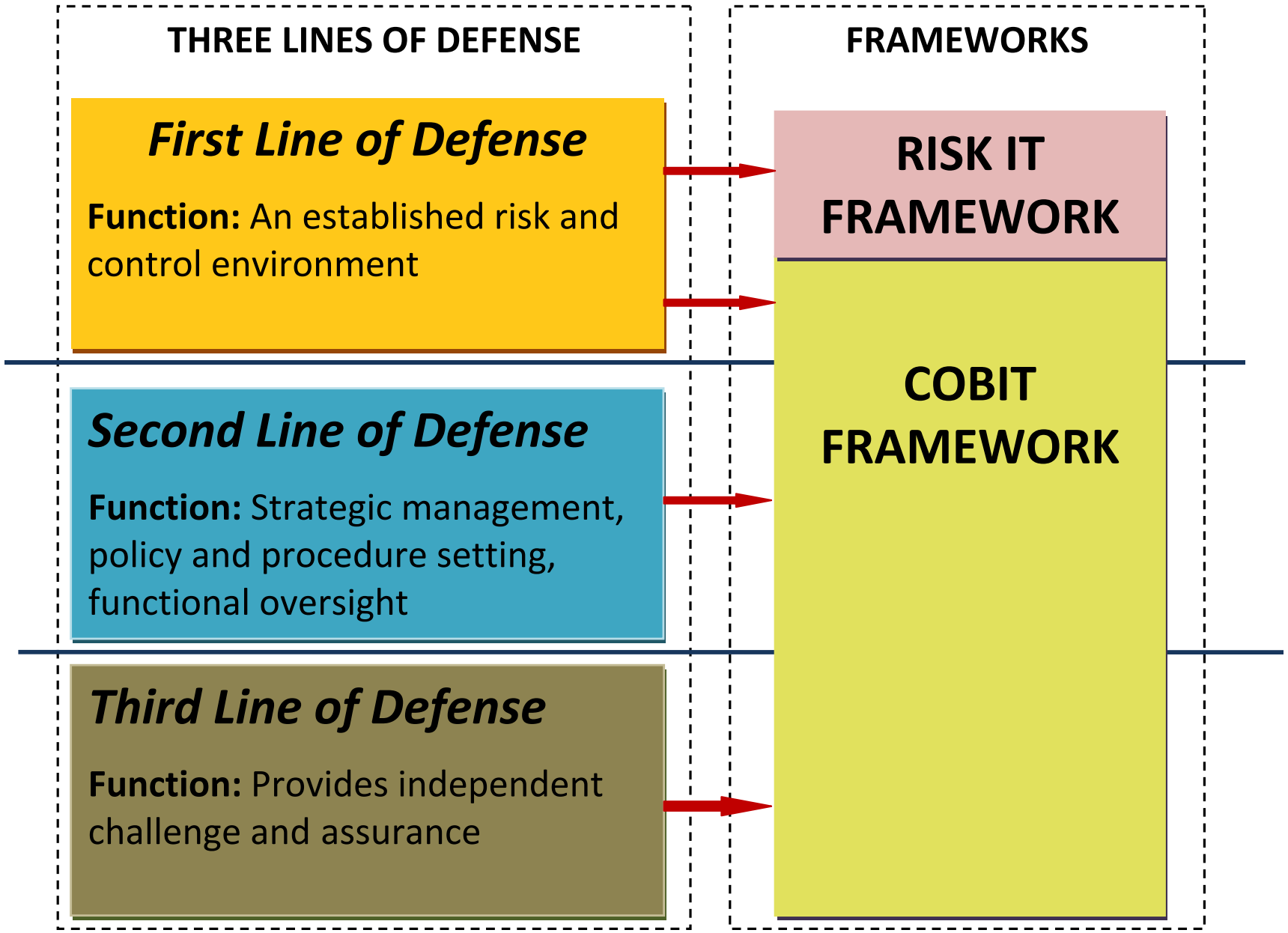
Responsibility: Independence assurance includes internal audit, external audit and other independent assurance providers, offers independent challenge to the levels of assurance provided by business operations and oversight functions.

Function: Provides independent challenge and assurance

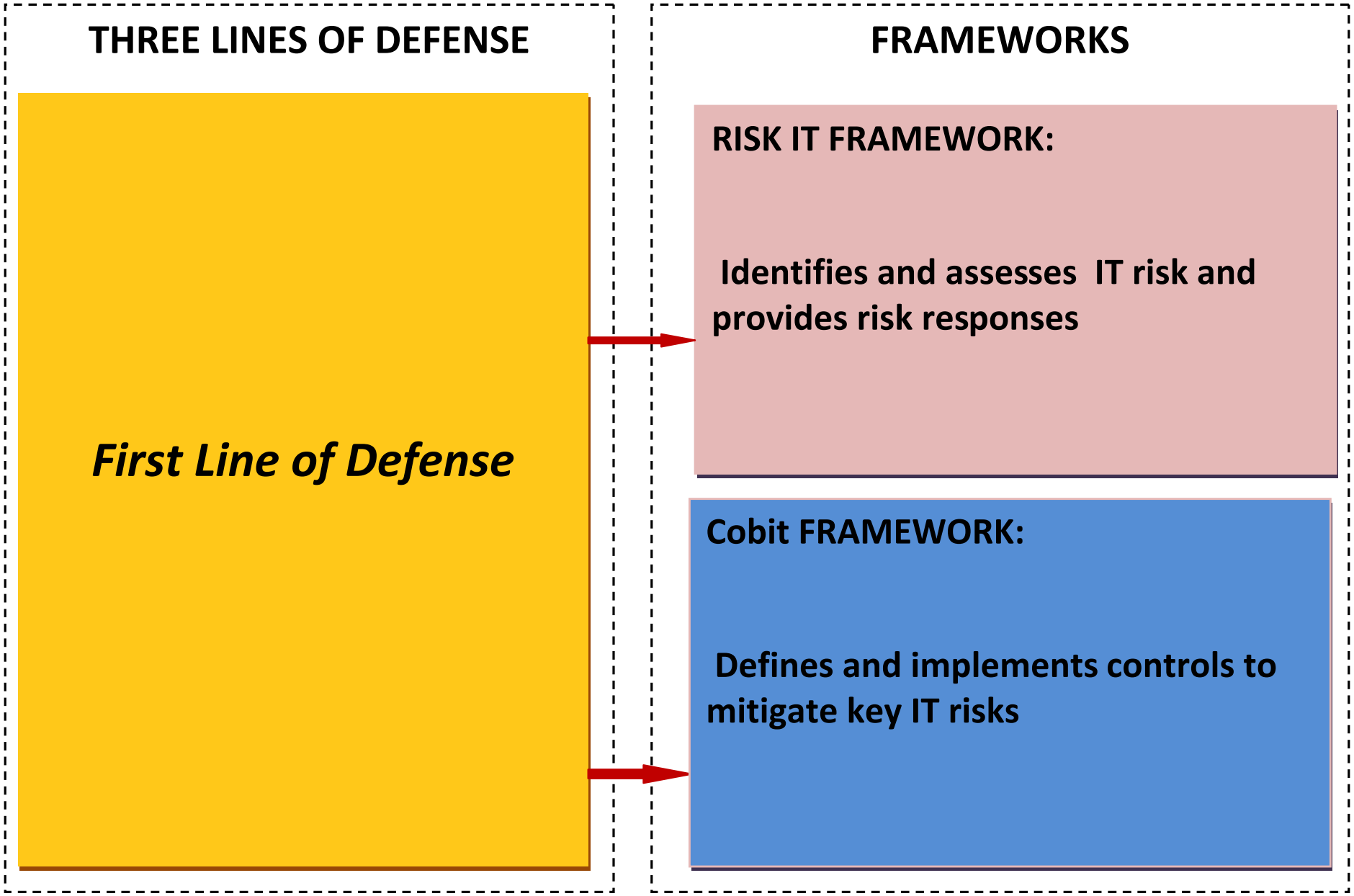
What is the relationship between Risk IT Framework and Cobit Framework

Cobit processes manage all IT-related activities within an enterprise. These processes deal with events internal and externally. These events could pose a risk to the enterprise and need to be assessed and responses developed. This risk dimension and how to manage it is the main subject of the Risk IT Framework. Results from implementing the Risk IT Framework will have an impact on some of the IT processes and/or the input of the IT processes.

How do the Risk IT Framework and Cobit fit into the Three Lines of Defense Model



First Line of Defense



What is Risk IT Framework?

- Risk IT framework defines , and is founded on, a number of guiding principles for effective management of IT risk.

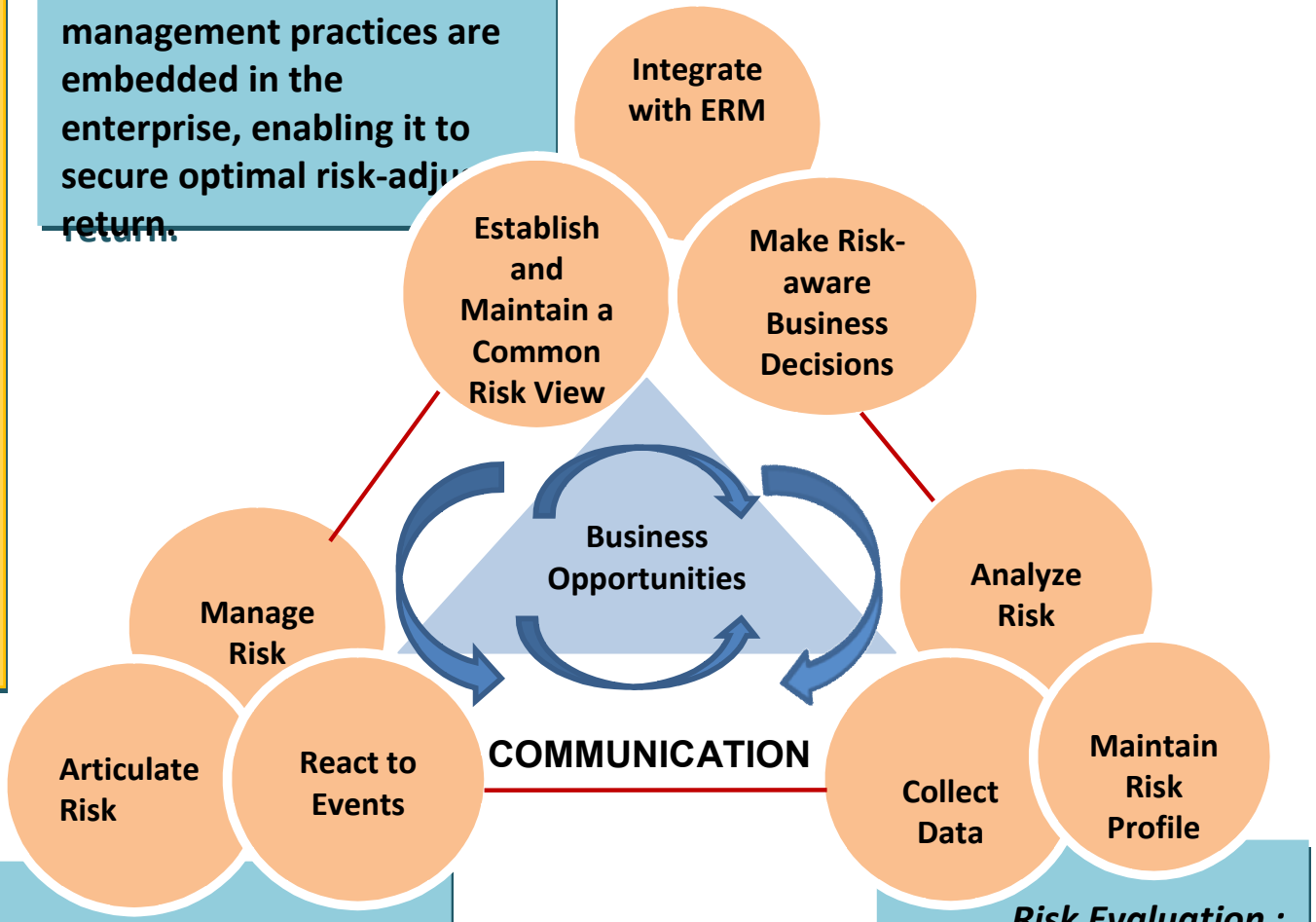
Risk IT Framework - components

Risk Governance (RG)
RG1 Establish and maintain a common risk view
RG2 Integrate with ERM
RG3 Make risk-aware business decisions

Risk Evaluation (RE)
RE1 Collect data
RE2 Analyse risk
RE3 Maintain risk profile

Risk Response (RR)
RR1 Articulate Risk
RR2 Manage risk
RR3 React to events

Risk Governance :
Ensures that IT risk management practices are embedded in the enterprise, enabling it to secure optimal risk-adju return.



Risk Response :
Ensure that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities

Risk Evaluation :
Ensure that IT-related risks and opportunities are identified, analyzed and presented in business terms

Risk Governance (RG) processes

RG1 Establish and maintain a common risk view

RG2 Integrate with ERM

RG3 Make risk-aware business decisions

Risk Universe

- Risk Universe defines boundaries of risk management activities and provides a structure for managing IT risk.
- It considers overall business objectives , business processes and their dependencies throughout the enterprise and describes which IT applications and infrastructures support the business objectives through provision of IT services.
- It also considers a life-cycle view of IT-related business activities,including transformation programmes, investments, projects and operations.

IT Risk Assessment

- A high level risk assessment performed to obtain initial view on overall IT risk

- Reason for assessment:
  - Identification of potentially high-risk areas
  - Overview of major risk factors

Enterprise IT Risk Assessment Form

Part1

Entity	
Entity strategic role and objectives	
Assessment date	
Assessor(s)	
Major business processes	
IT infrastructure and applications supporting major business processes	
Important dependencies	
Part II – Risk Factor Assessment	

Risk Factor (Reference)	Assessment	Rating	Comment
External Factors			
Industry/Competition			
Internal Environment			
Complexity of IT			
Risk Management Capability(Risk IT)			
Risk Governance			
IT Management Capability (Cobit)			
Plan and Organise			

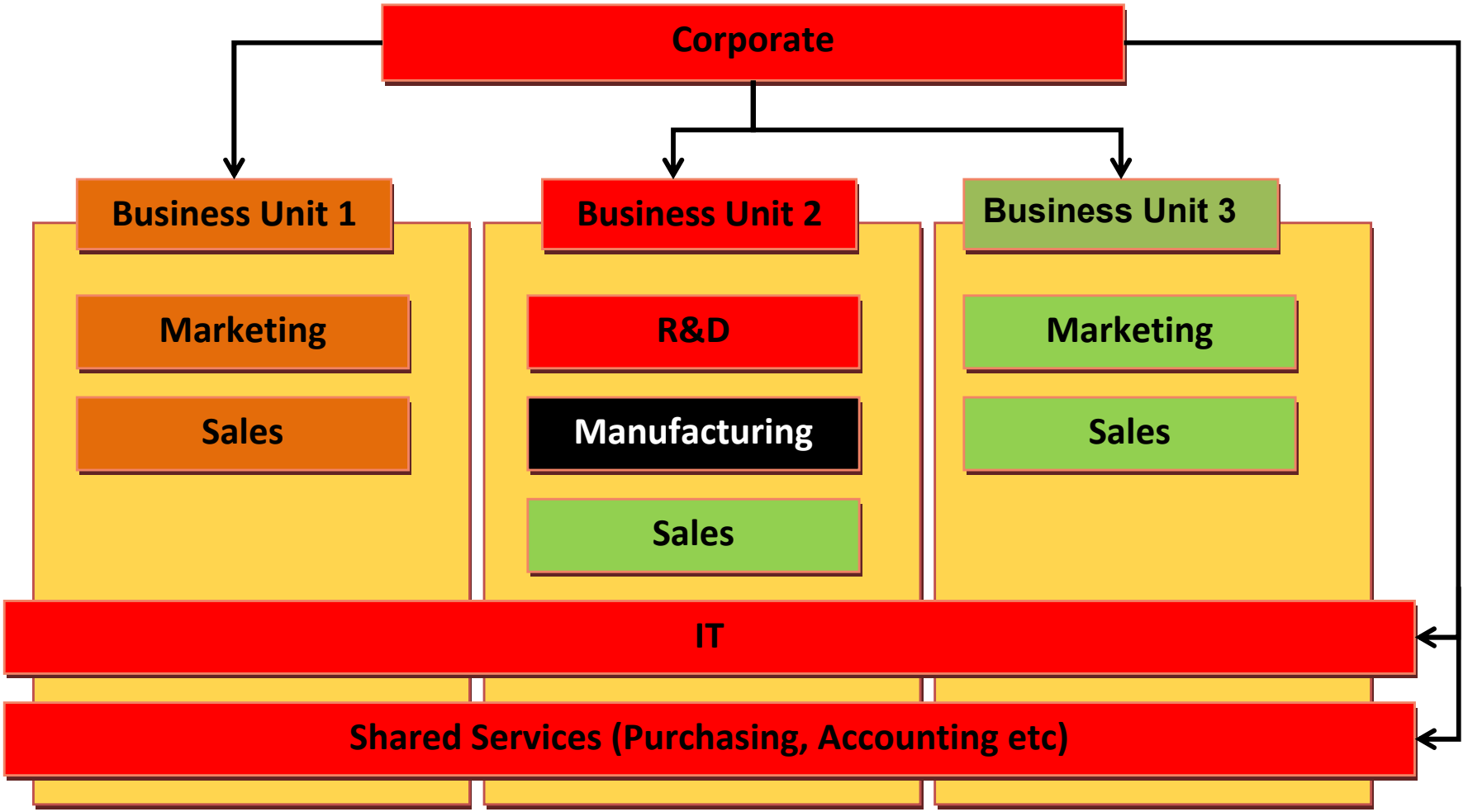
Overall l high-level IT risk rating (based on results of the assessment of all risk factors below)	**Low** Entity is marginally dependent on IT and/or IT risk is well controlled	**Medium** Entity is dependent on IT and/or some IT risks are not well controlled	**High** Entity is very dependent on IT and/or significant IT risk management deficiencies exist	**Very High** Entity is critically dependent on IT and/or very significant IT risk management issues exist

Scoping of IT Risk Management

Scoping includes activities to decide:

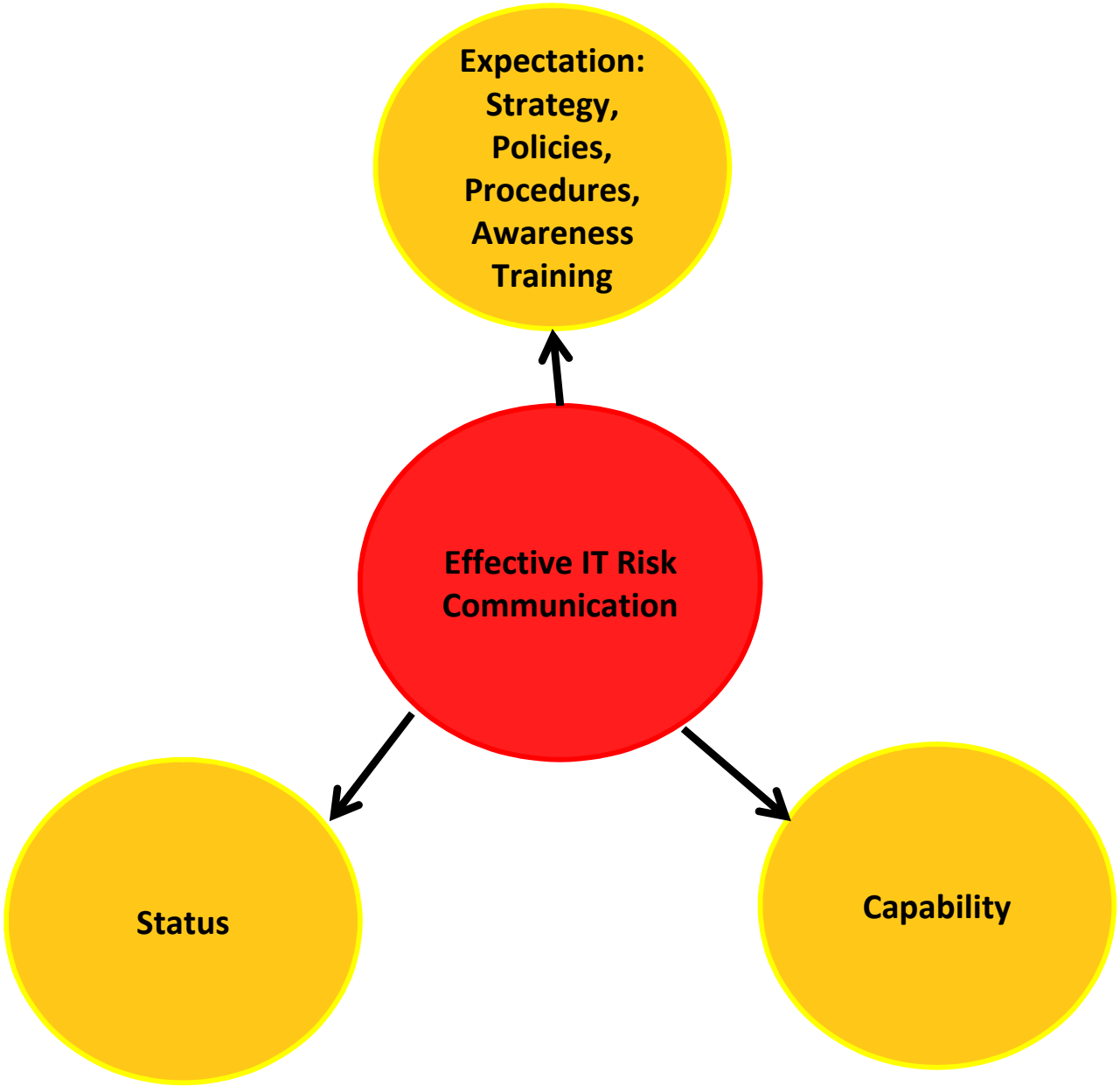
- Which entities in the risk universe will be subject to risk management activities
- The expected breadth and depth of risk management activities, including risk analysis and reporting

Result of Enterprise IT Risk Assessment



The chart above brings together all business lines , functional areas and risk importance.

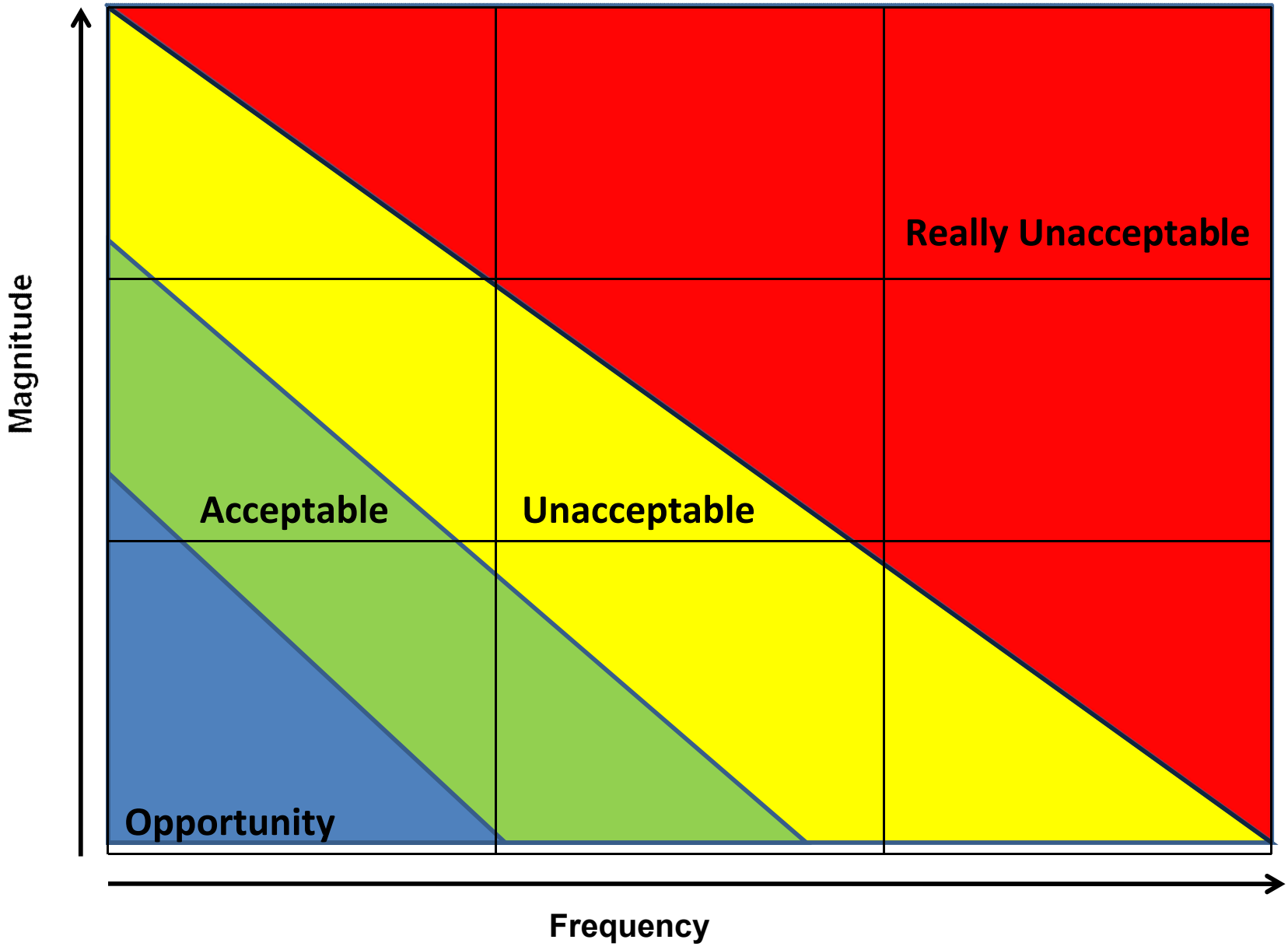
IT Risk Communication



Risk Appetite & Risk Tolerance

- What is Risk Appetite?
- What is Risk Tolerance?

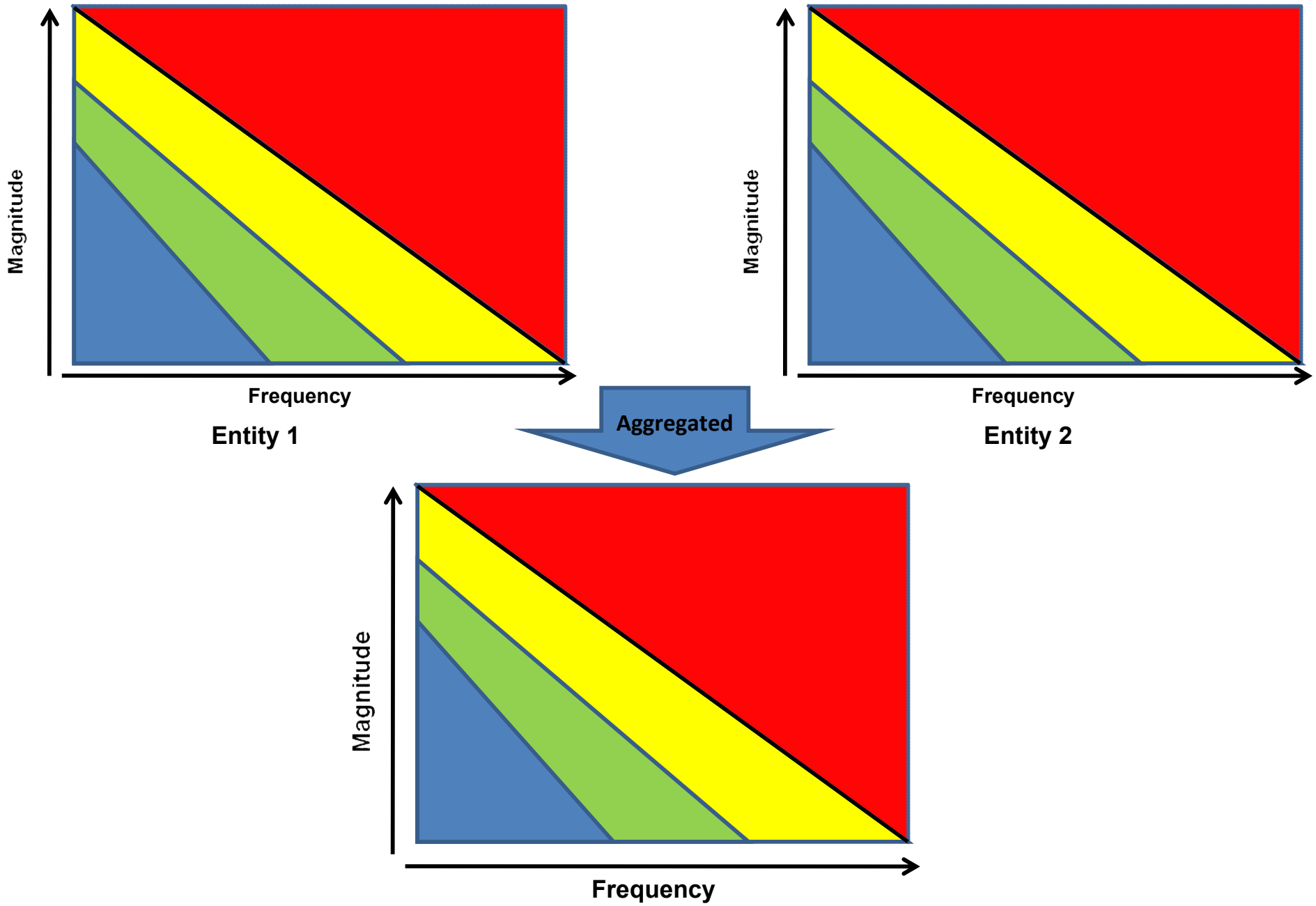
Risk Map Indicating Risk Appetite Bands



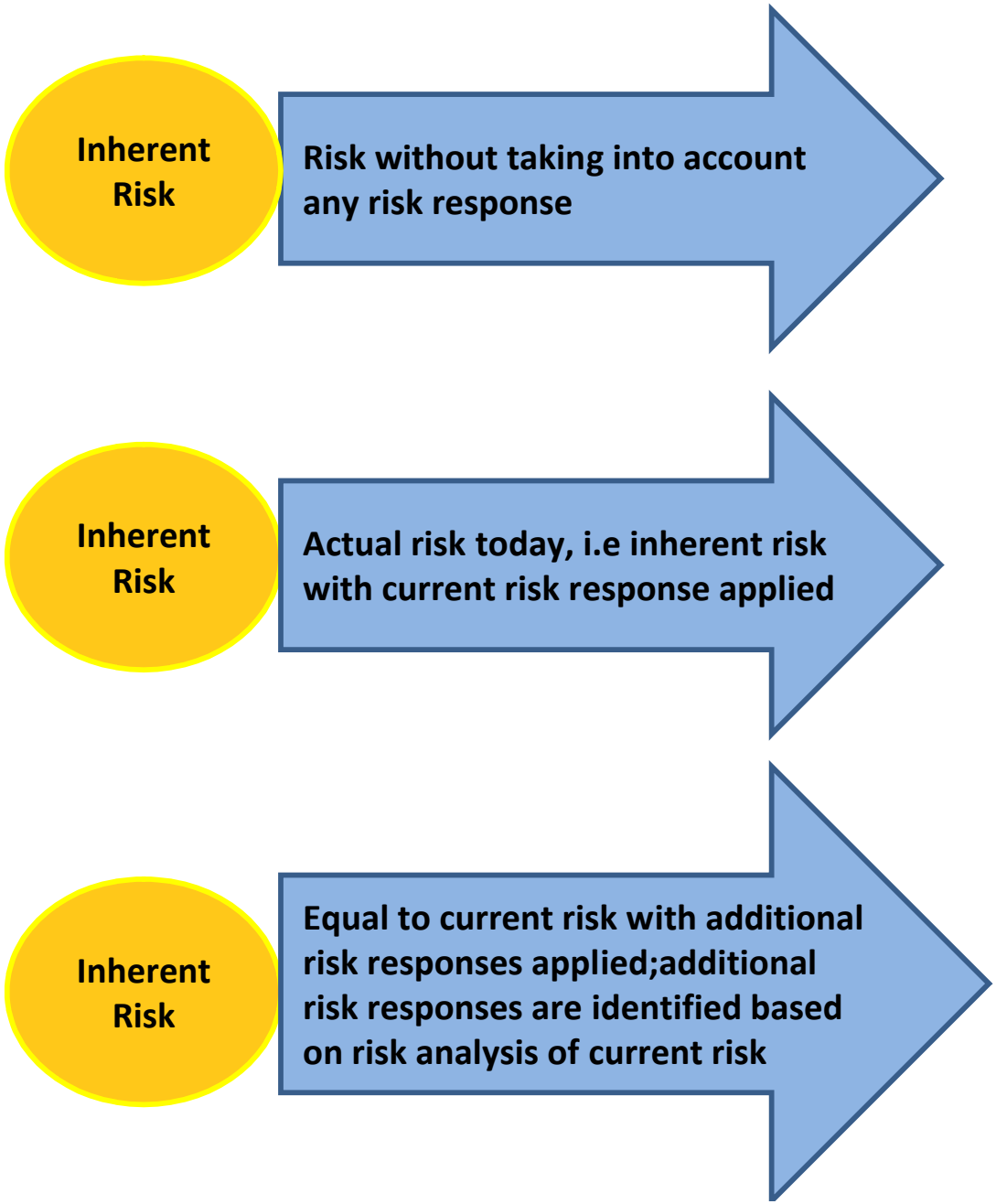
Risk Aggregation & Risk Profile

- What is the Risk Aggregation?
- What is the Risk Profile ?

Risk Aggression (continued)



Inherent Risk, Current Risk and Residual Risk



Risk Evaluation (RE) -Processes

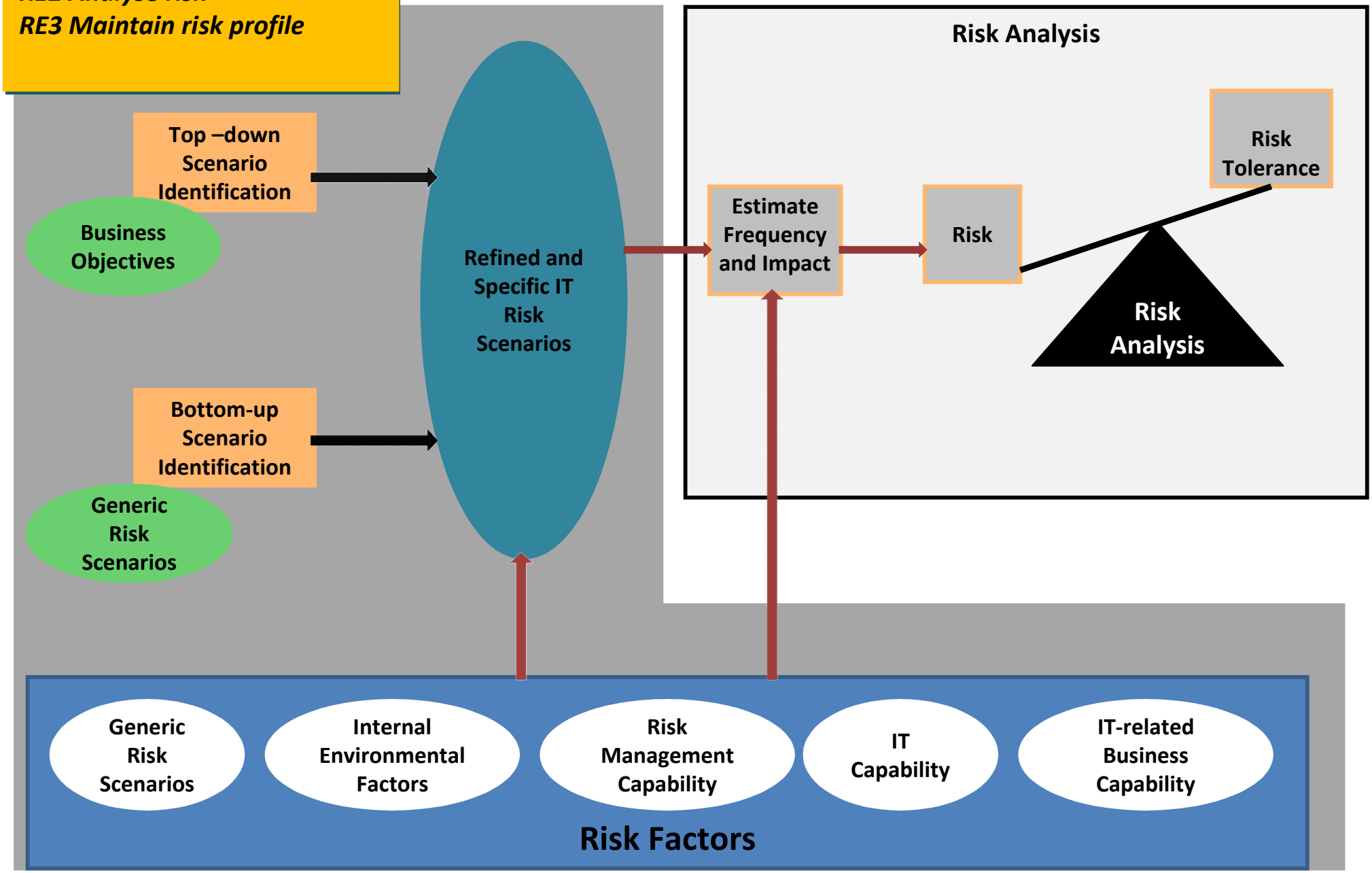
RE1 Collect data

RE2 Analyse risk

RE3 Maintain risk profile

Risk Evaluation

Risk Evaluation (RE) -Processes
RE1 Collect data
RE2 Analyse risk
RE3 Maintain risk profile



Risk Indicators and Risk Reporting

- What is a Risk Indicator ?
- What is Risk Reporting ?

Risk Responses (RG) processes

RR1 Articulate Risk

RR2 Manage risk

RR3 React to events

Risk Responses

The four types of responses are:

- Risk Avoidance
- Risk Sharing/Transfer
- Risk Acceptance
- Risk Reduction/ Mitigation

Risk Responses

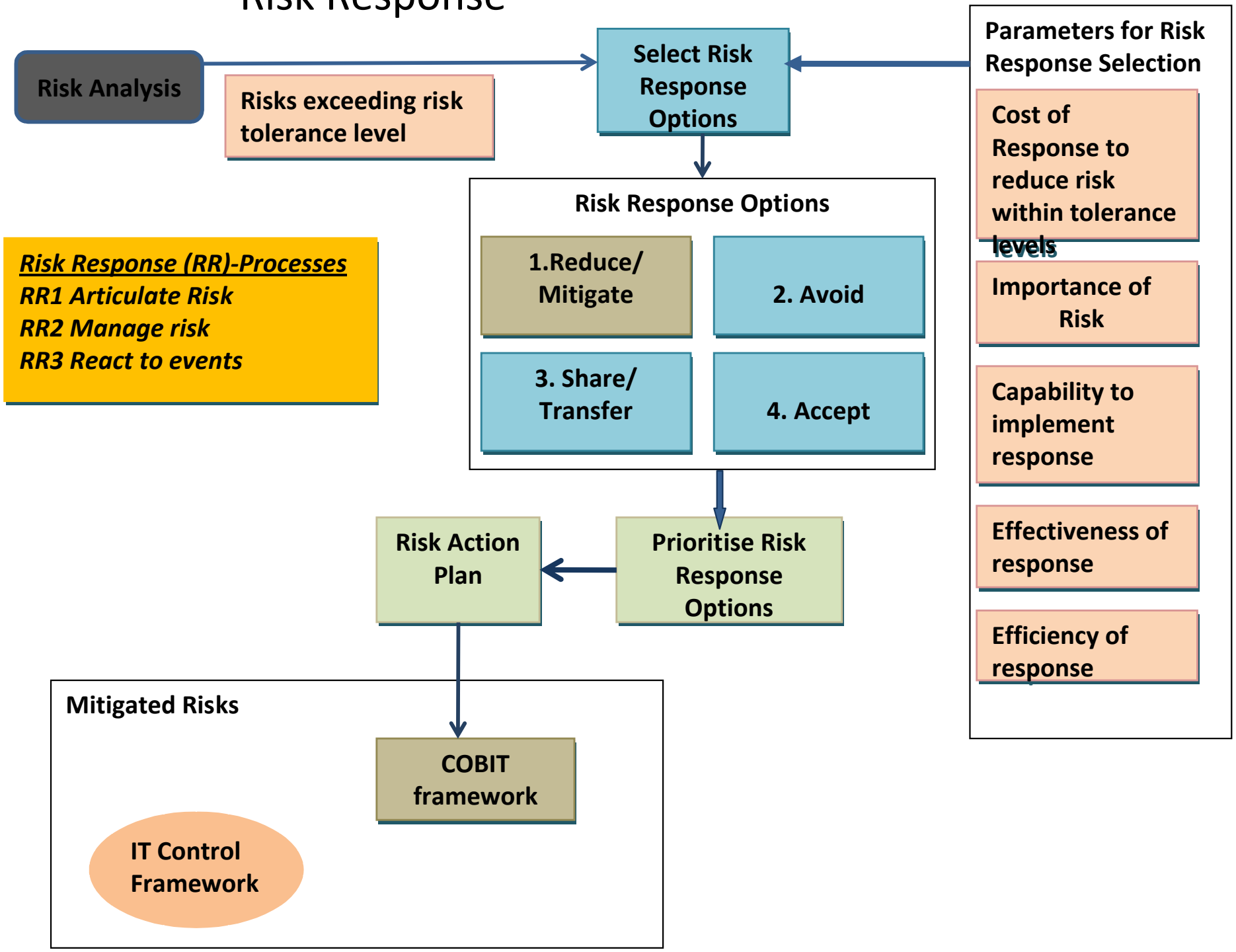
•**Risk Avoidance** which means exiting activities or conditions that give rise to risk. Risk Avoidance applies when no other risk response is adequate.

•**Risk Sharing/Transfer** which means reducing risk frequency or impact by transferring or sharing a portion of the risk. Examples are insurance and outsourcing.

•**Risk Acceptance** which means that no action is taken relative to a particular risk, and loss is accepted when or if it occurs. This is different from being ignorant of risk but that the accepting risk assumes that the risk is known and an informed decision has been made by management to accept the risk.

•**Risk Reduction/ Mitigation** which means that action is taken to detect risk, followed by action to reduce the frequency and/or impact of a risk. Mitigated risks can be managed through a control framework for IT governance such as Cobit.

Risk Response



Mapping Key IT Risks(Risk IT) to Key Processes (Cobit) - continued

High-level Risk	IT Management Capabilities			
	Plan and Organise (PO)	Acquire and Implement(AI)	Deliver and Support(DS)	Monitor and Evaluate(ME)
Logical Attacks	PO2, PO3		DS5, DS12	

Mapped Cobit Processes

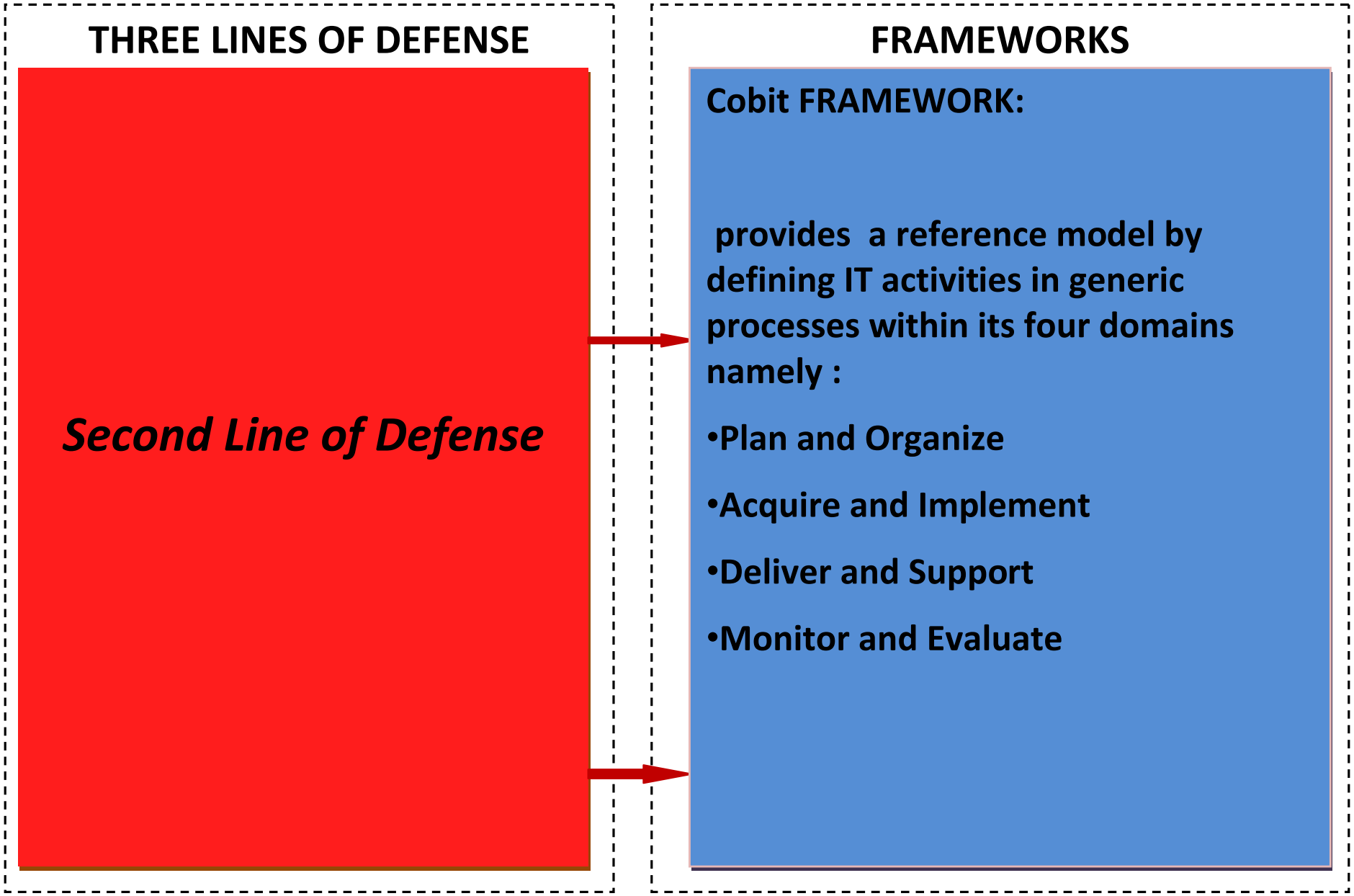
PO2 Define the Information Architecture

PO3 Determine Technological Direction

DS 12 Manage the Physical Environment

DS5 Ensure System Security

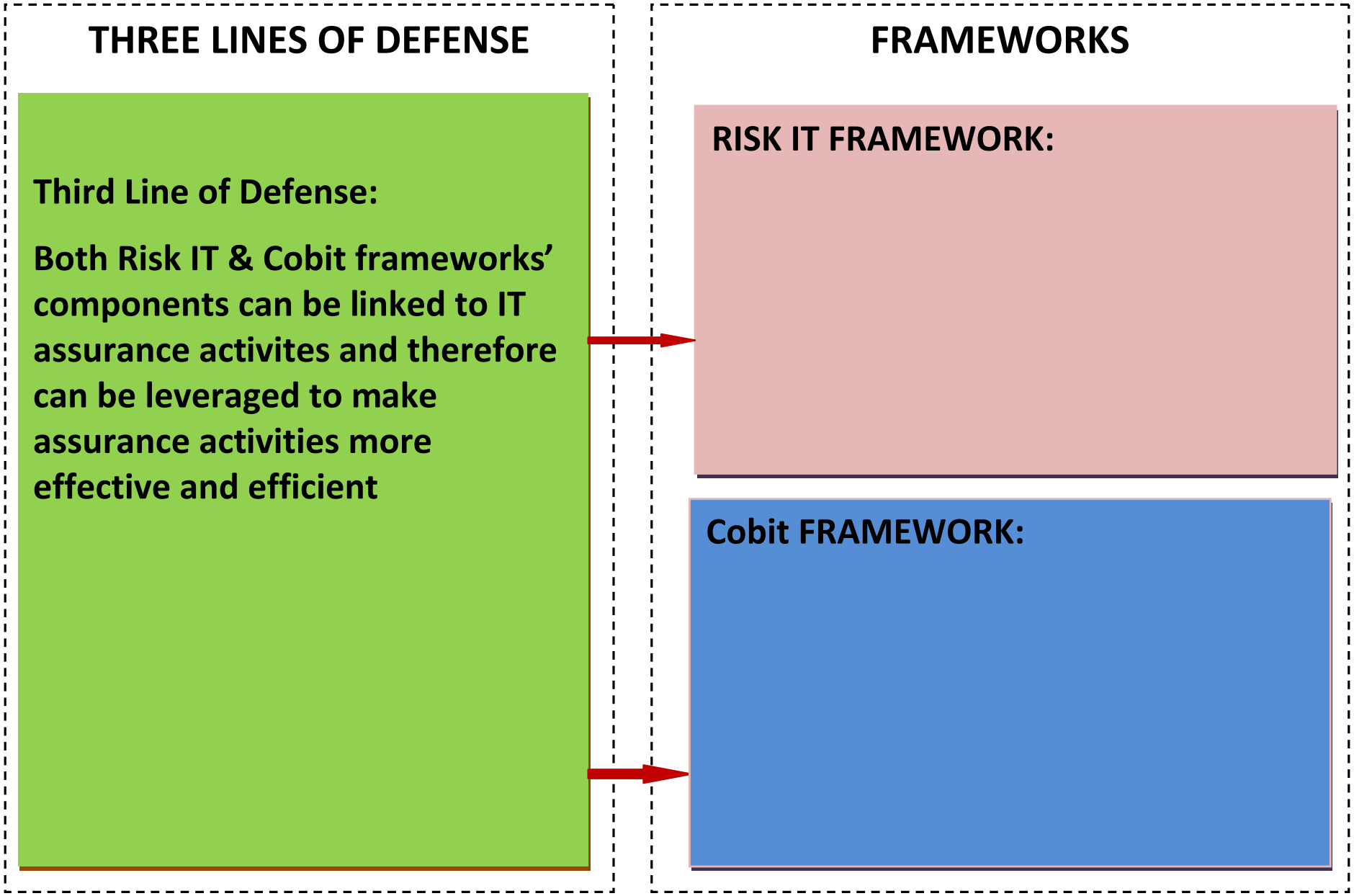
Second Line of Defense



Cobit Processes

- **How is Cobit implemented within the Second Line of Defense?**

Three Line of Defense



Mapping IT Assurance Activities to Risk IT and Cobit Frameworks

IT Assurance Activities	Risk IT	Cobit
Perform a quick risk assessment	√	
Assess threat,vulnerability and business impact	√	
Diagnose operational and project risk	√	
Plan risk-based assurance initiatives	√	√
Identify critical IT processes based on value drivers		√
Assess process maturity		√
Scope and plan assurance initiatives		√
Select the control objectives for critical processes		√
Customise control objectives		√
Build a detailed assurance programme		√
Test and evaluate controls		√
Substantiate risk		√
Report assurance conclusions		√
Self-assess process maturity		√
Self-assess controls.		√

For further questions, **Ronke Oyemade** can be reach at :

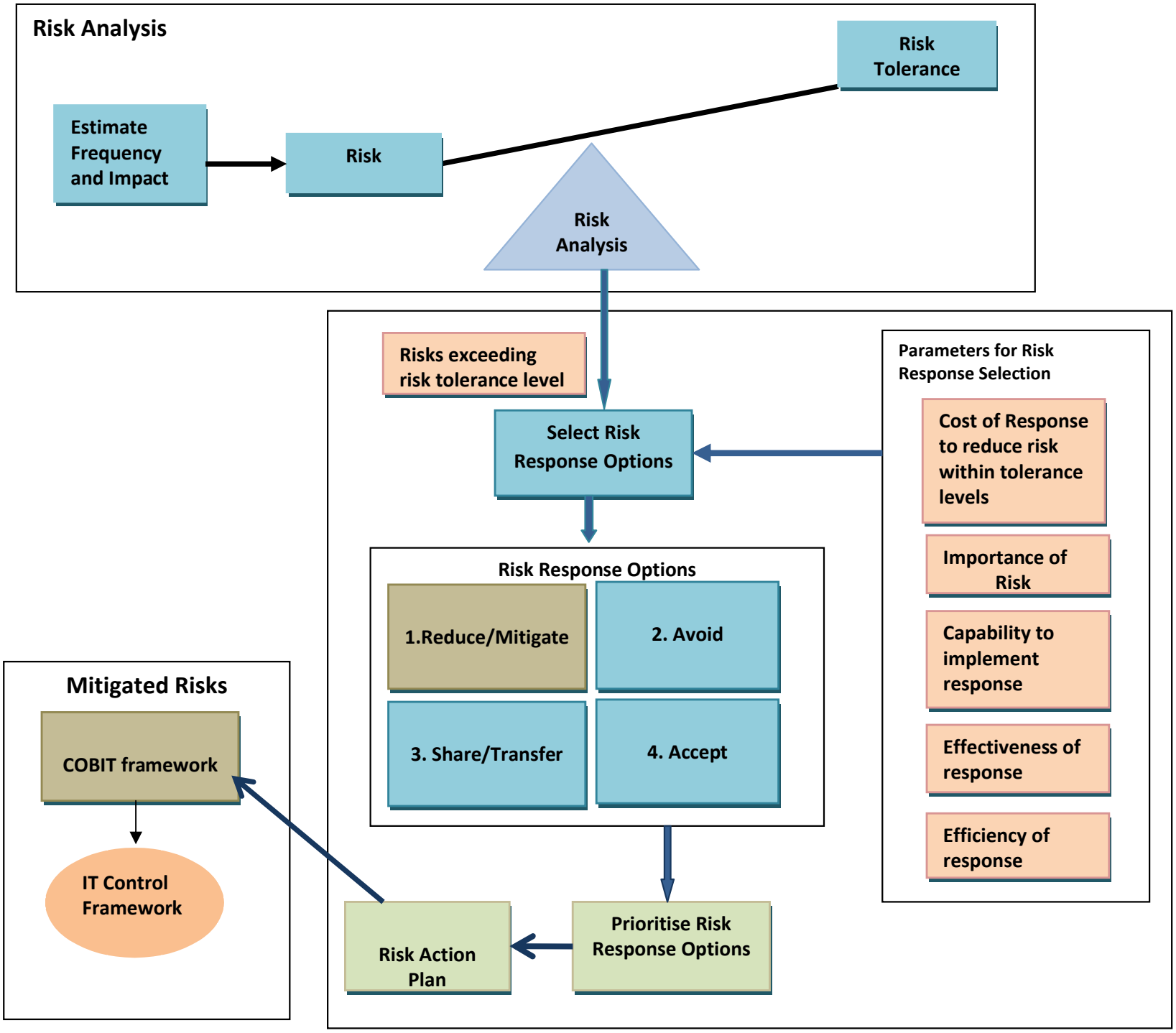
ronke.oyemade@strategicglobalconsult.com
information@strategicglobalconsult.com
strategicglobalconsult@gmail.com
Tel: 678-7681228
www.strategicglobalconsult.com

Wrap-up

- Questions ???

Appendices

Appendix 1: Risk IT Framework



Appendix 2: Mapping Key IT Risks(Risk IT) to Key Processes (Cobit)

High-level Risk	IT Management Capabilities			
	Plan and Organise (PO)	Acquire and Implement(AI)	Deliver and Support(DS)	Monitor and Evaluate(ME)
Logical Attacks	PO2, PO3		DS5, DS12	

PO2 Define the Information Architecture

The information systems function creates and regularly updates a business information model and defines the appropriate systems to optimise the use of this information. This encompasses the development of a corporate data dictionary with the organisation's data syntax rules, data classification scheme and security levels. This process improves the quality of management decision making by making sure that reliable and secure information is provided, and it enables rationalising information systems resources to appropriately match business strategies. This IT process is also needed to increase accountability for the integrity and security of data and to enhance the effectiveness and control of sharing information across applications and entities.

PO3 Determine Technological Direction

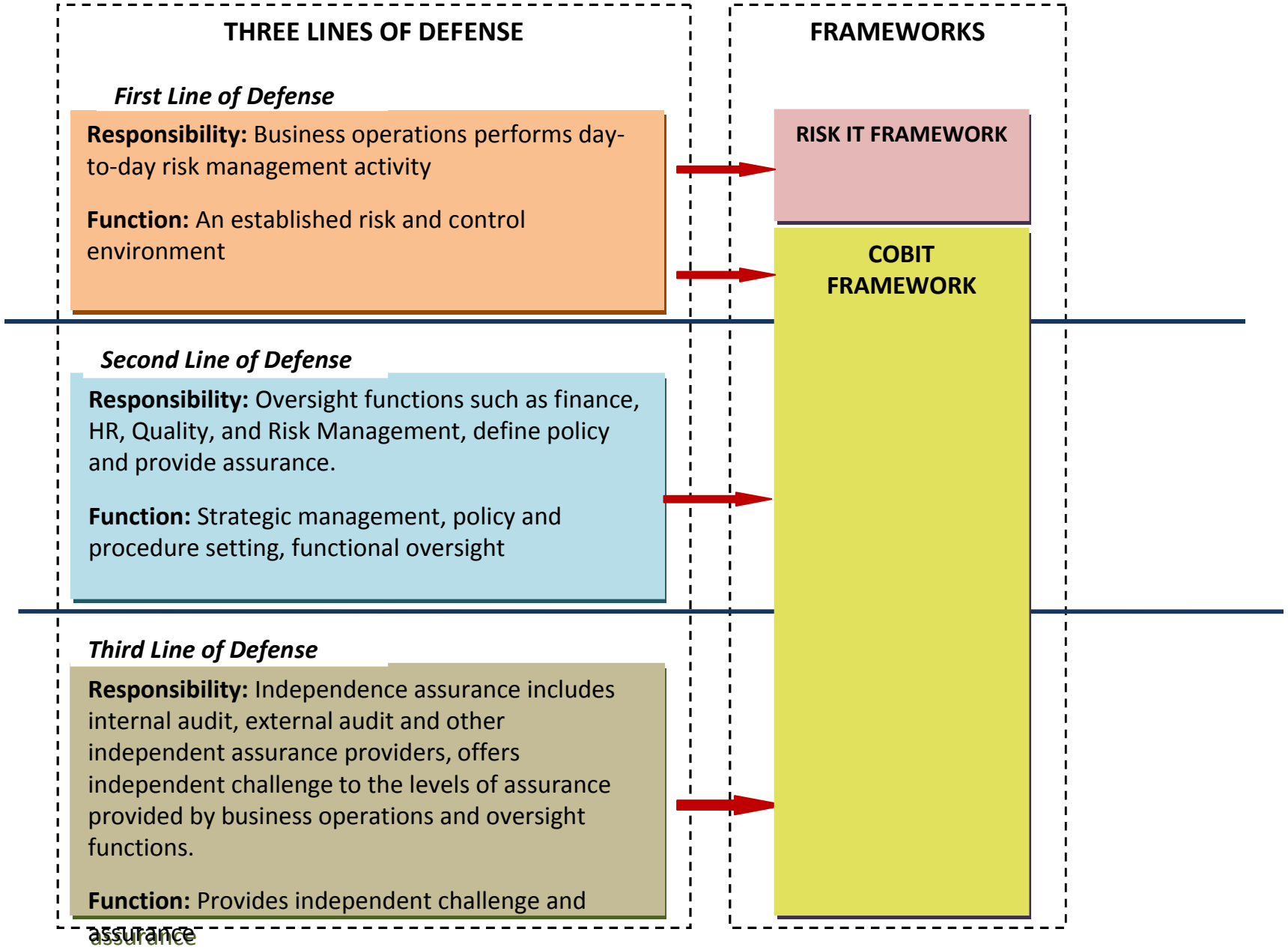
The information services function determines the technology direction to support the business. This requires the creation of a technological infrastructure plan and an architecture board that sets and manages clear and realistic expectations of what technology can offer in terms of products, services and delivery mechanisms. The plan is regularly updated and encompasses aspects such as systems architecture, technological direction, acquisition plans, standards, migration strategies and contingency. This enables timely responses to changes in the competitive environment, economies of scale for information systems staffing and investments, as well as improved interoperability of platforms and applications.

Appendix 2: Mapping Key IT Risks(Risk IT) to Key Processes (Cobit) - continued

DS 12 Manage the Physical Environment
Protection for computer equipment and personnel requires well-designed and well-managed physical facilities. The process of managing the physical environment includes defining the physical site requirements, selecting appropriate facilities, and designing effective processes for monitoring environmental factors and managing physical access. Effective management of the physical environment reduces business interruptions from damage to computer equipment and personnel.

DS5 Ensure System Security
The need to maintain the integrity of information and protect IT assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibilities, policies, standards, and procedures. Security management also includes performing security monitoring and periodic testing and implementing corrective actions for identified security weaknesses or incidents. Effective security management protects all IT assets to minimise the business impact of security vulnerabilities and incidents.

Appendix 3: Overview of The Lines of Defense, Risk IT and Cobit frameworks



END