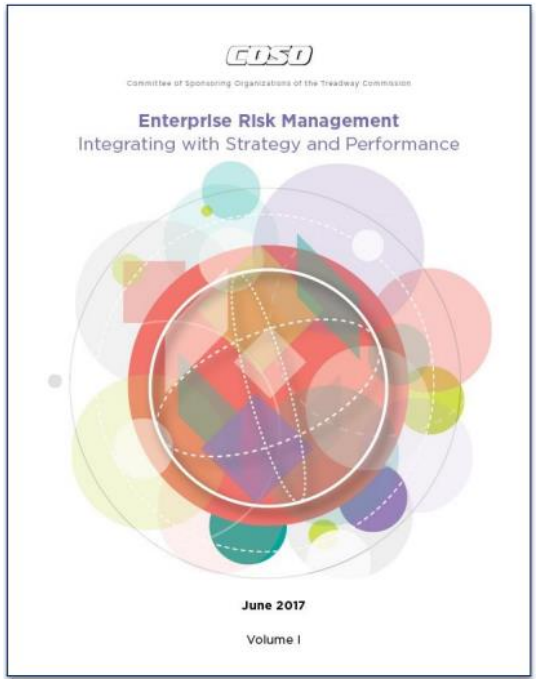
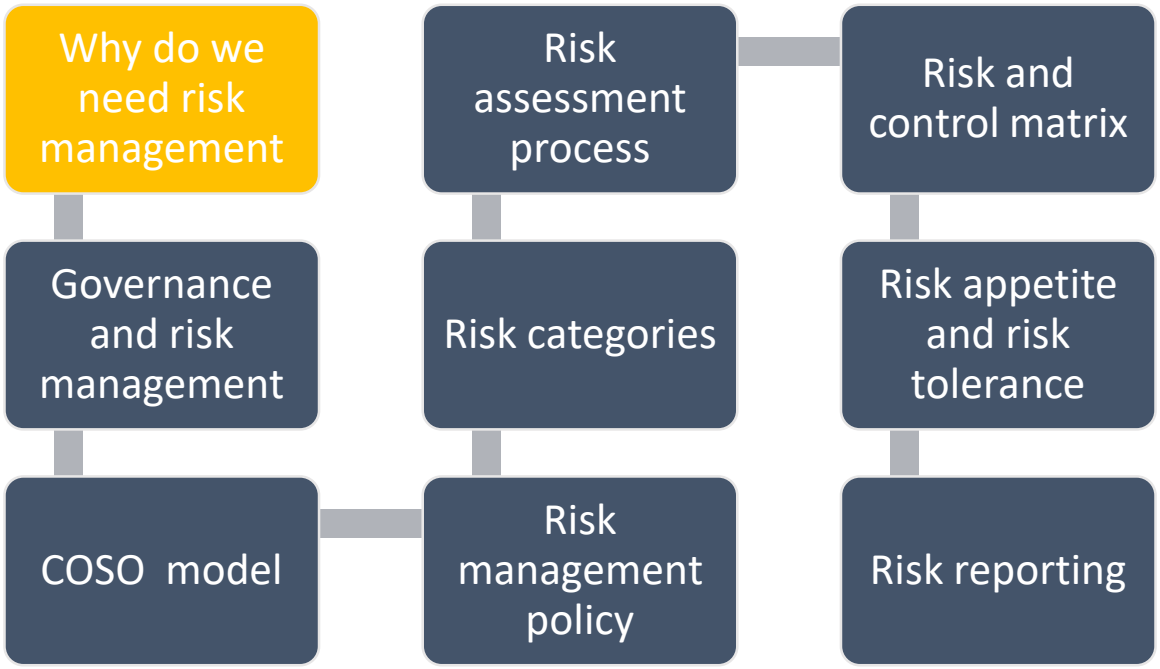


Risk management

Deon van der Westhuizen
deon@nsa.edu.za

Structure of session



Need for risk management

Risk management creates and protects strategic value to all stakeholders

Risk management is an integral part of all organizational processes

Risk management is part of decision making

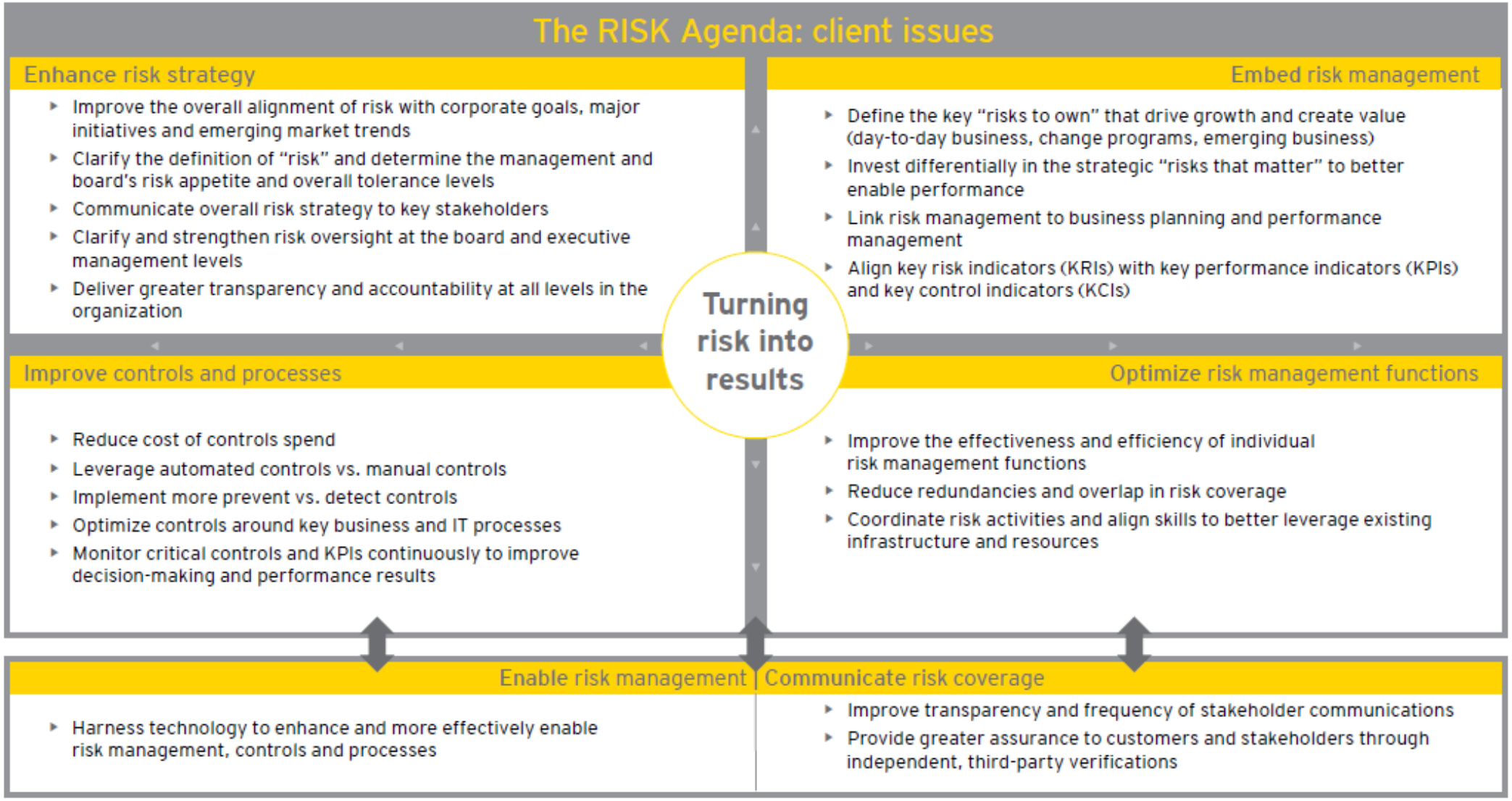
Risk management explicitly addresses uncertainty and opportunity

Risk management is systematic, structured and timely

Risk management facilitates continual improvement of the organization


Structure of session
Why do we need risk management
Governance and risk management
COSO model
Risk assessment process
Risk categories
Risk management policy
Risk and control matrix
Risk appetite and risk tolerance
Risk reporting

The Risk Agenda




Structure of session
Why do we need risk management
Governance and risk management
COSO model
Risk assessment process
Risk categories
Risk management policy
Risk and control matrix
Risk appetite and risk tolerance
Risk reporting

Best practice risk management frameworks

20 key principles within each of the five components

Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues improvement in Enterprise Risk Management

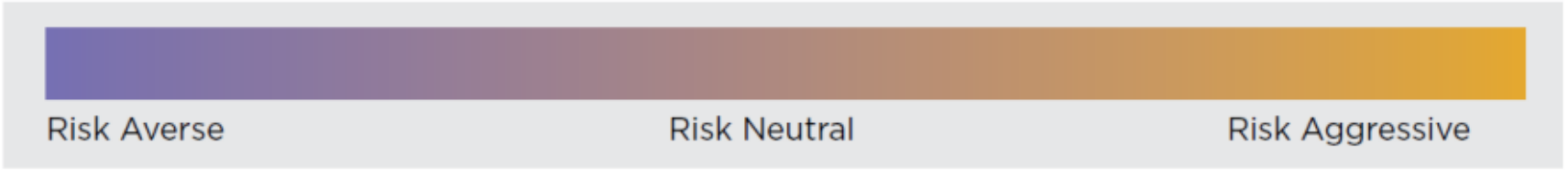
Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

Graphic has stronger ties to the business model

Importance of culture

- Addresses the growing focus, attention and Importance of culture within enterprise risk management
- Influences all aspects of enterprise risk management
- Explores culture within the broader context of overall core
- Depicts culture behavior within a risk spectrum



- Explores the possible effects of culture on decision making
- Explores the alignment of culture between individual and entity behavior

- Explores strategy from three different perspectives:
  - The possibility of strategy and business objectives not aligning with mission, vision and values
  - The implications from the strategy chosen
  - Risk to executing the strategy

Integration= improved decisions = enhanced performance

- It helps organizations to:
  - Anticipate risks earlier or more explicitly, opening up more options for managing the risks
  - Identify and pursue existing and new opportunities
  - Respond to deviations in performance more quickly and consistently
  - Develop and report a more comprehensive and consistent portfolio view of risk
  - Improve collaboration, trust, and information sharing

PETROLEUM *Fund*
Looking after your Petroleum Interests

Links to performance

- Enables the achievement of strategy by actively managing risk and performance
- Focuses on how risk is integral to performance by:
  - Exploring how enterprise risk management practices support the identification and assessment of risks that impact performance
  - Discussing tolerance for variations in performance
- Manages risk in the context of achieving strategy and business objectives – not as individual risks

KPI's and KRI's

Key Performance Indicators (KPIs) help a firm see how it is performing in relation to its strategic goals and objectives.

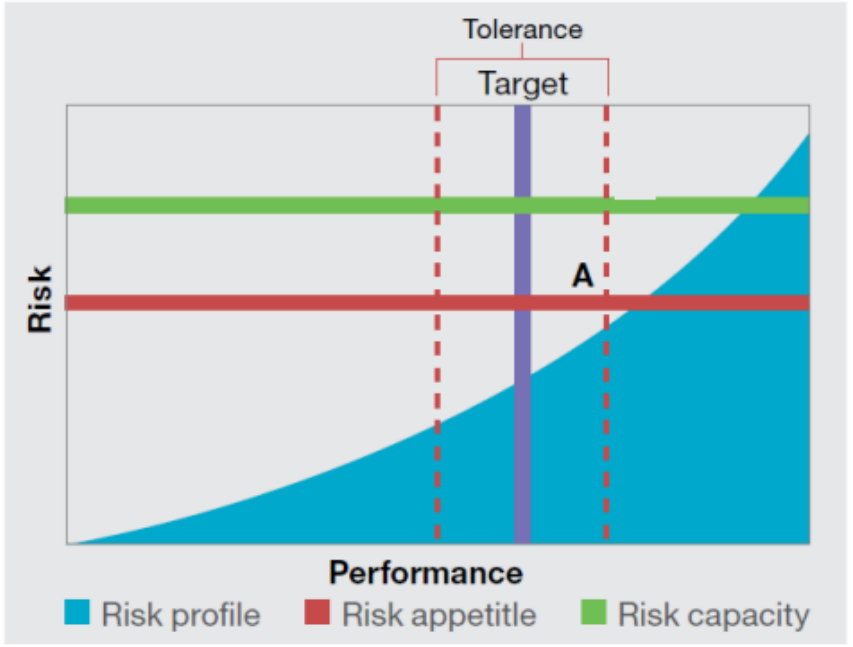
Key Risk Indicators (KRIs) are leading indicators of risk to business performance, giving early warning about potential risk event

Use KRIs to monitor risks are in the areas such as:

- natural catastrophe risks (as % of group shareholder equity)
- asset-liability matching (duration mismatch)
- strategic asset allocation (% allowed in investment category)
- credit risk (weighted average credit rating)
- other risks specific to business or functional areas

Risk versus performance

- Introduces a new depiction referred to as a risk profile
- Incorporates:
  - Risk
  - Performance
  - Risk appetite
  - Risk capacity
- Offers a comprehensive view of risk and enables more risk-aware decision making



- The framework provides a complete depiction of how to build a risk profile in an appendix

Design, build and implementation of Key Risk Indicators

Design

- Establish extent of existing management information and other data flows – indicators in place if applicable
- Identify committees, forums, management meetings etc currently in place that can be used to discuss risk and control issues on an ongoing basis
- Define and document roles and responsibilities of risk and control owners

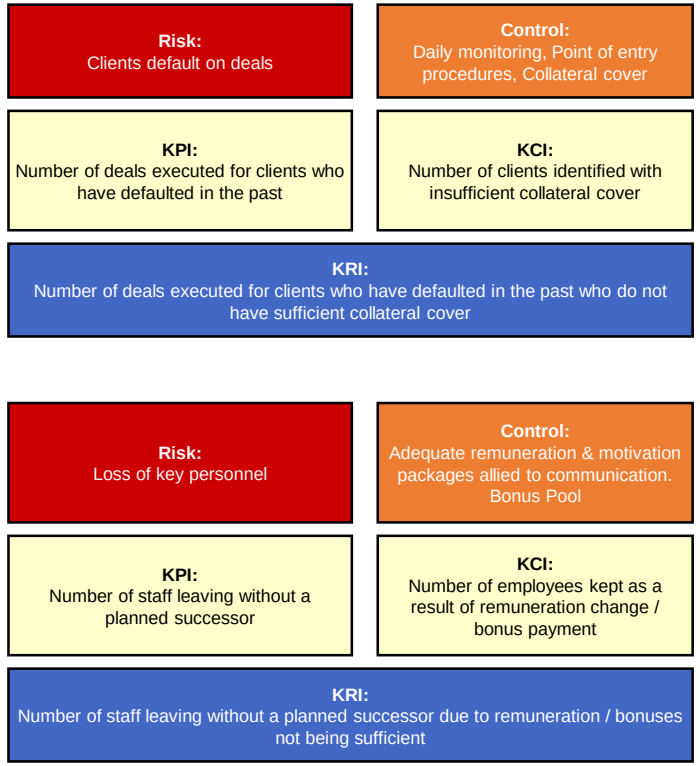
Build Process

- Assign ownership for risks and controls
- Communication with risk and control owners relating to their ongoing responsibilities
- Carry out workshops with all risk and control owners to design indicators to be put in place
- Define how existing information flows and committees etc are to be used to minimise additional workload
- Risk and control owners refine the indicator monitoring process
- Overall analysis of indicators for gaps and dual coverage
- Design reporting protocols

Ongoing Operation of Process

- Design review mechanism (i.e. Corporate Risk department or Internal Audit, etc.)
- Create storage mechanism for information
- Perform ongoing consistency checks of indicators set up across the organisation

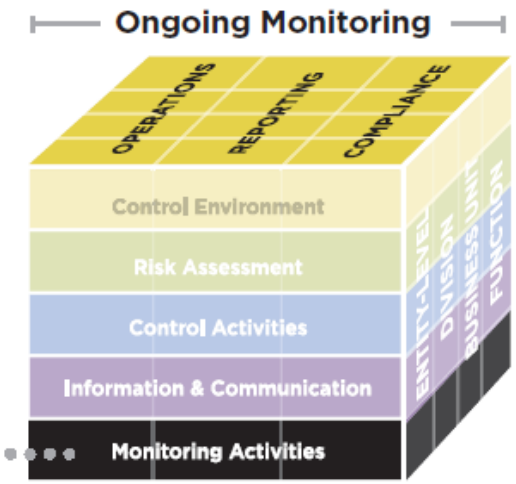
Example KPI, KCI and KRIs



Risk aware decision-making

Second line of defense

Figure 5. COSO and the 2nd Line of Defense

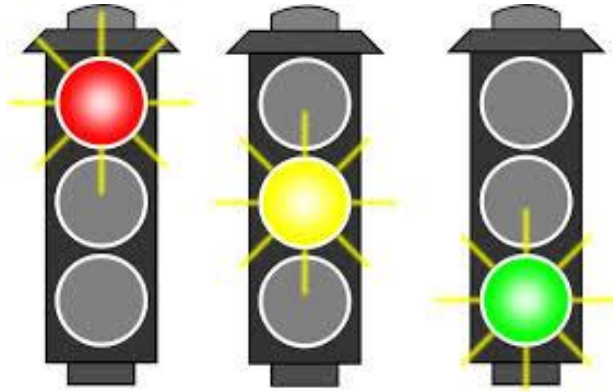


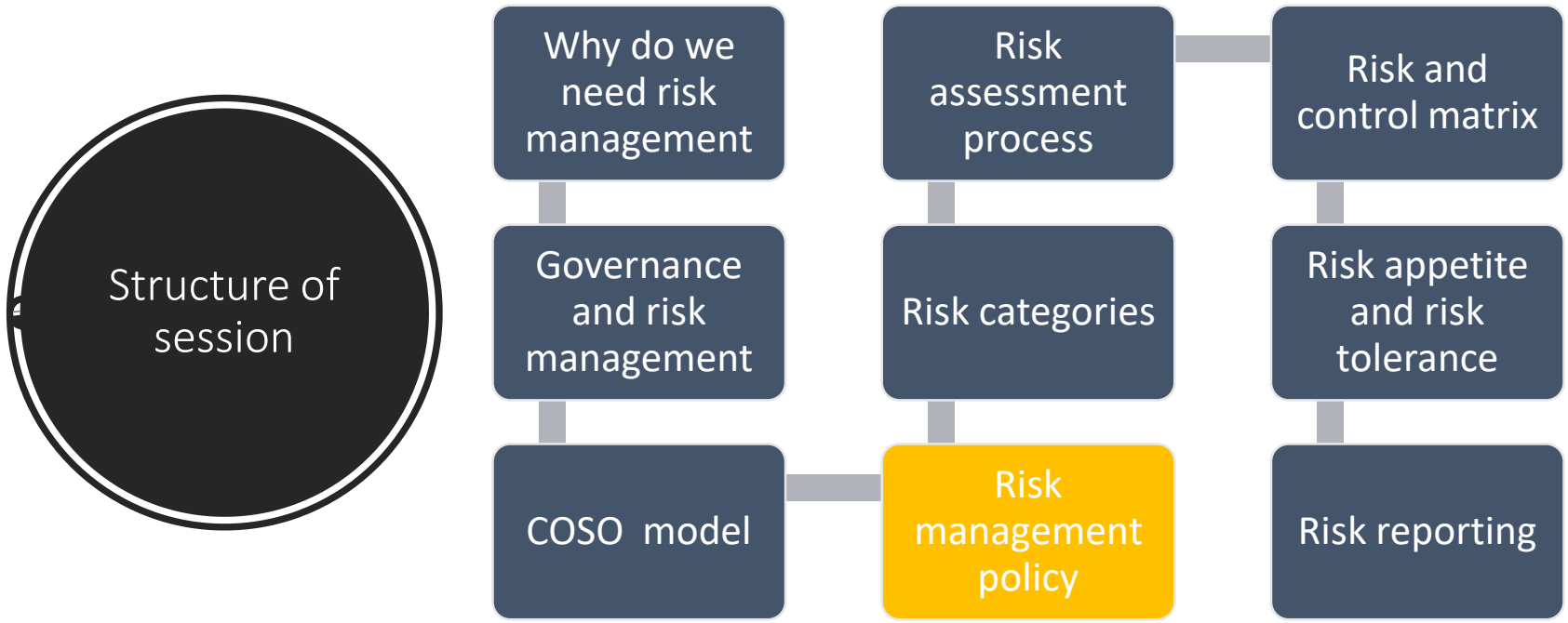
Monitoring Activities

16. Conducts ongoing and/or separate evaluations
17. Evaluates and communicates deficiencies

2nd Line of Defense

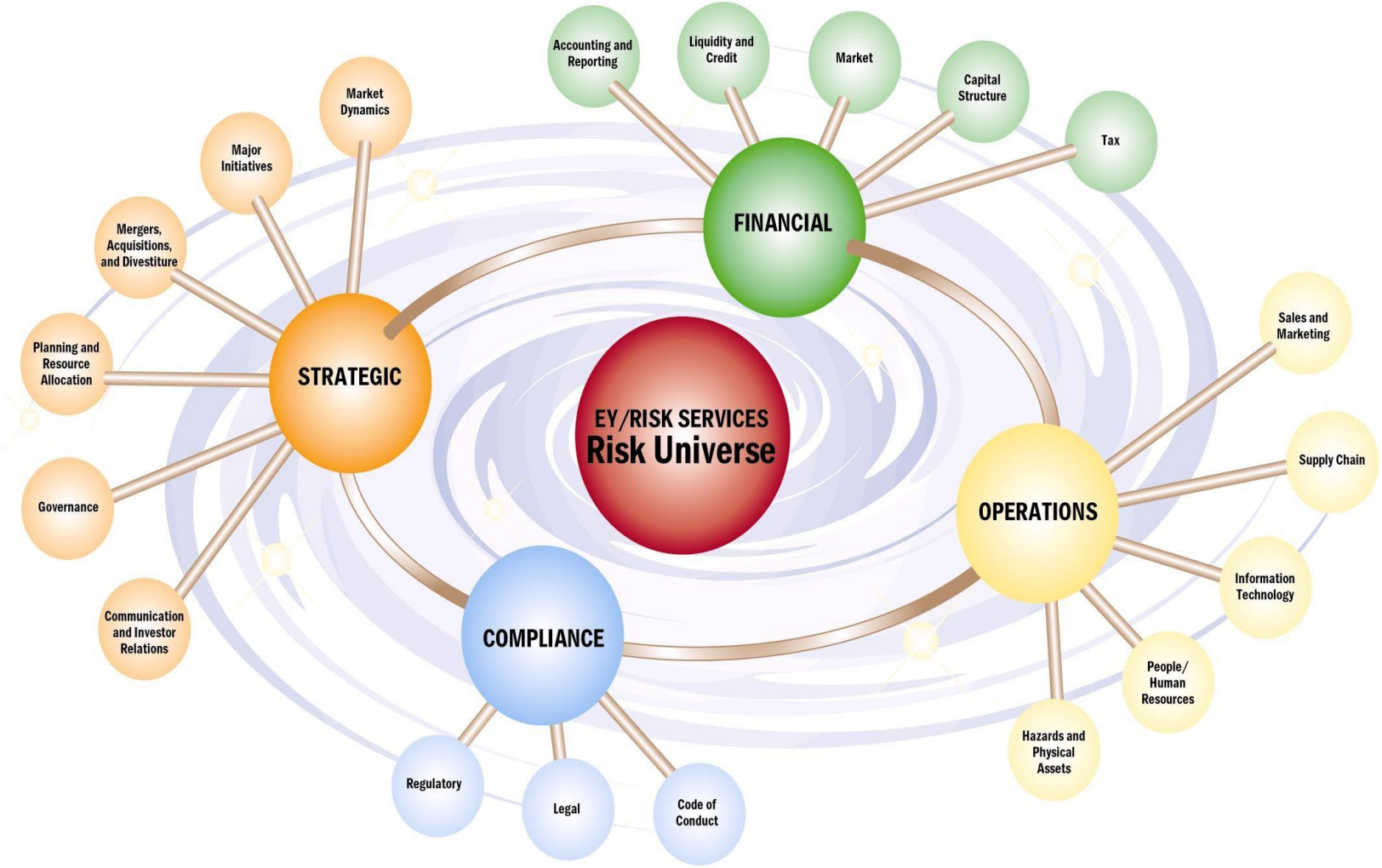
- Financial Control
- Security
- Risk Management
- Quality
- Inspection
- Compliance




Structure of session
Why do we need risk management
Governance and risk management
COSO model
Risk assessment process
Risk categories
Risk management policy
Risk and control matrix
Risk appetite and risk tolerance
Risk reporting


Structure of session
Why do we need risk management
Governance and risk management
COSO model
Risk assessment process
Risk categories
Risk management policy
Risk and control matrix
Risk appetite and risk tolerance
Risk reporting

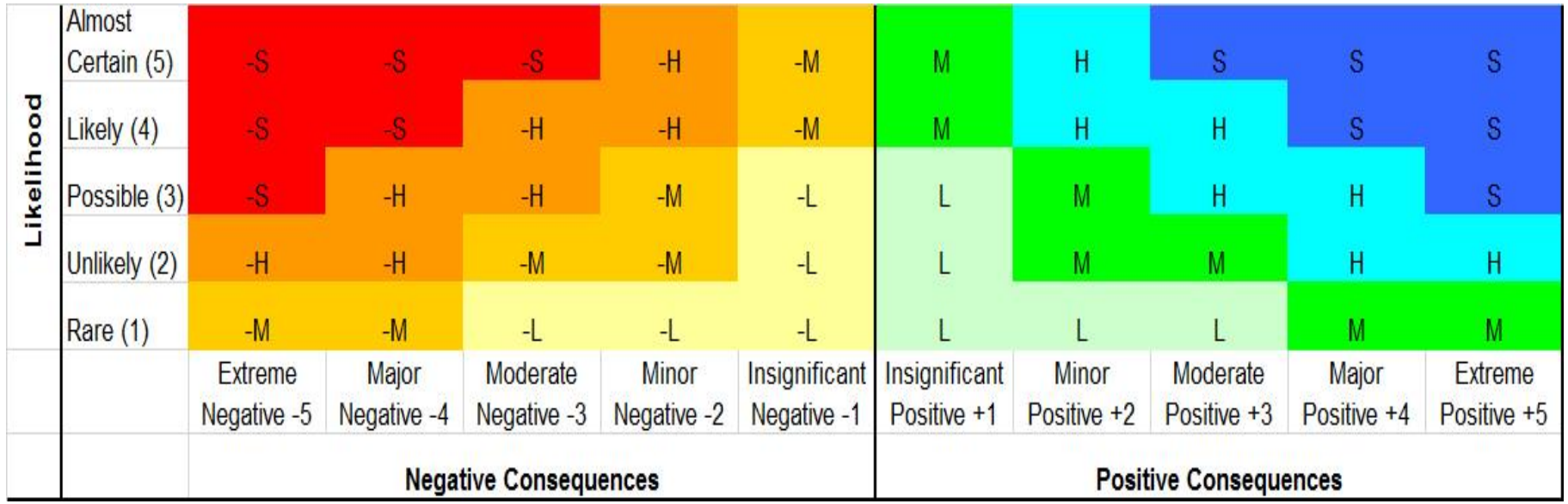
Risk universe



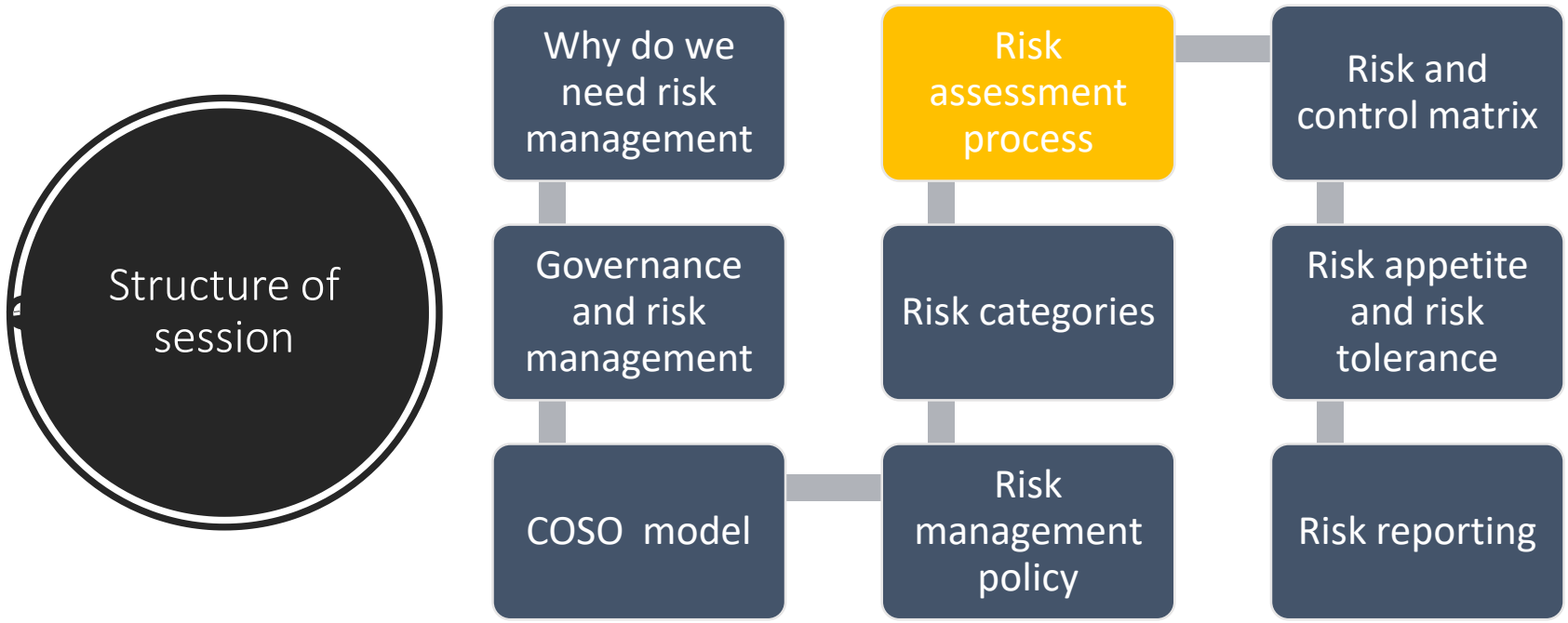
Risk Management

- Identifying areas of threat to the business
- Assessing the potential impacts and managing these
- Growth and continued existence of the business

Risk versus opportunity

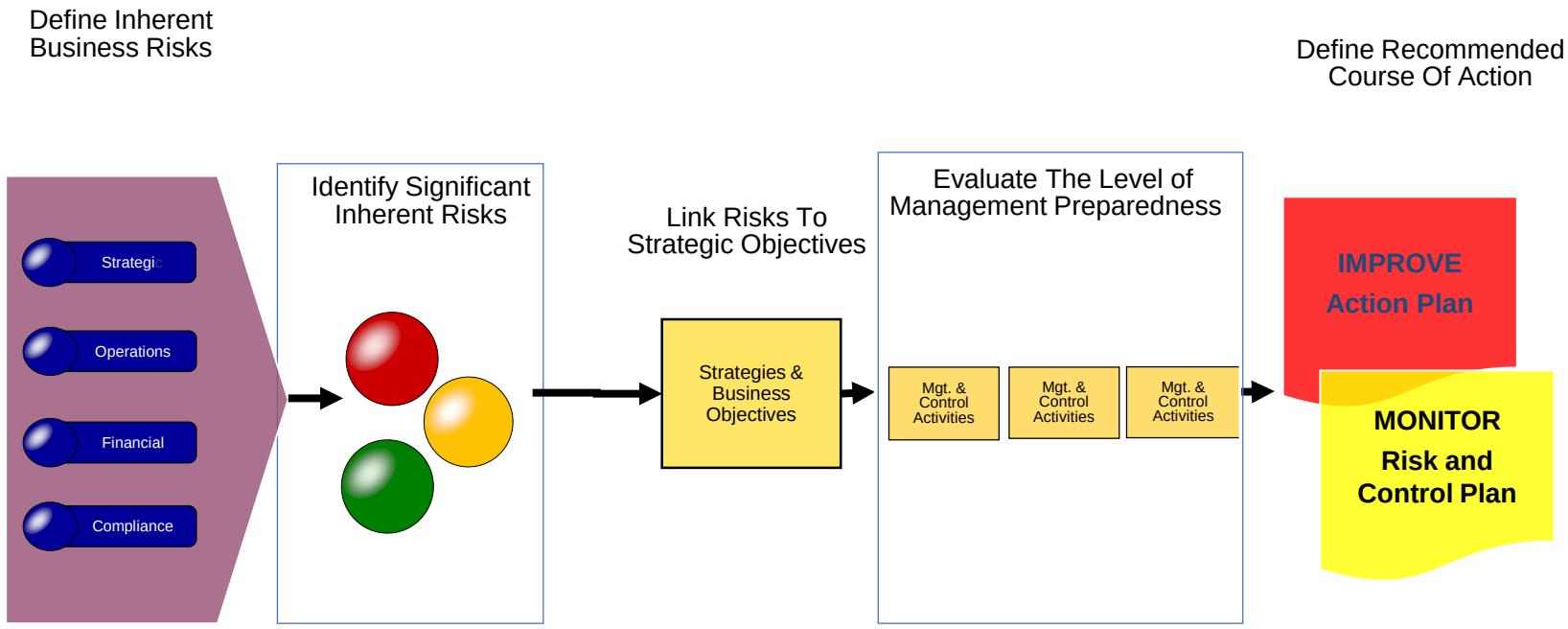


Likelihood											
	Almost Certain (5)	-S	-S	-S	-H	-M	M	H	S	S	S
	Likely (4)	-S	-S	-H	-H	-M	M	H	H	S	S
	Possible (3)	-S	-H	-H	-M	-L	L	M	H	H	S
	Unlikely (2)	-H	-H	-M	-M	-L	L	M	M	H	H
	Rare (1)	-M	-M	-L	-L	-L	L	L	L	M	M
		Extreme Negative -5	Major Negative -4	Moderate Negative -3	Minor Negative -2	Insignificant Negative -1	Insignificant Positive +1	Minor Positive +2	Moderate Positive +3	Major Positive +4	Extreme Positive +5
		Negative Consequences					**Positive Consequences**				

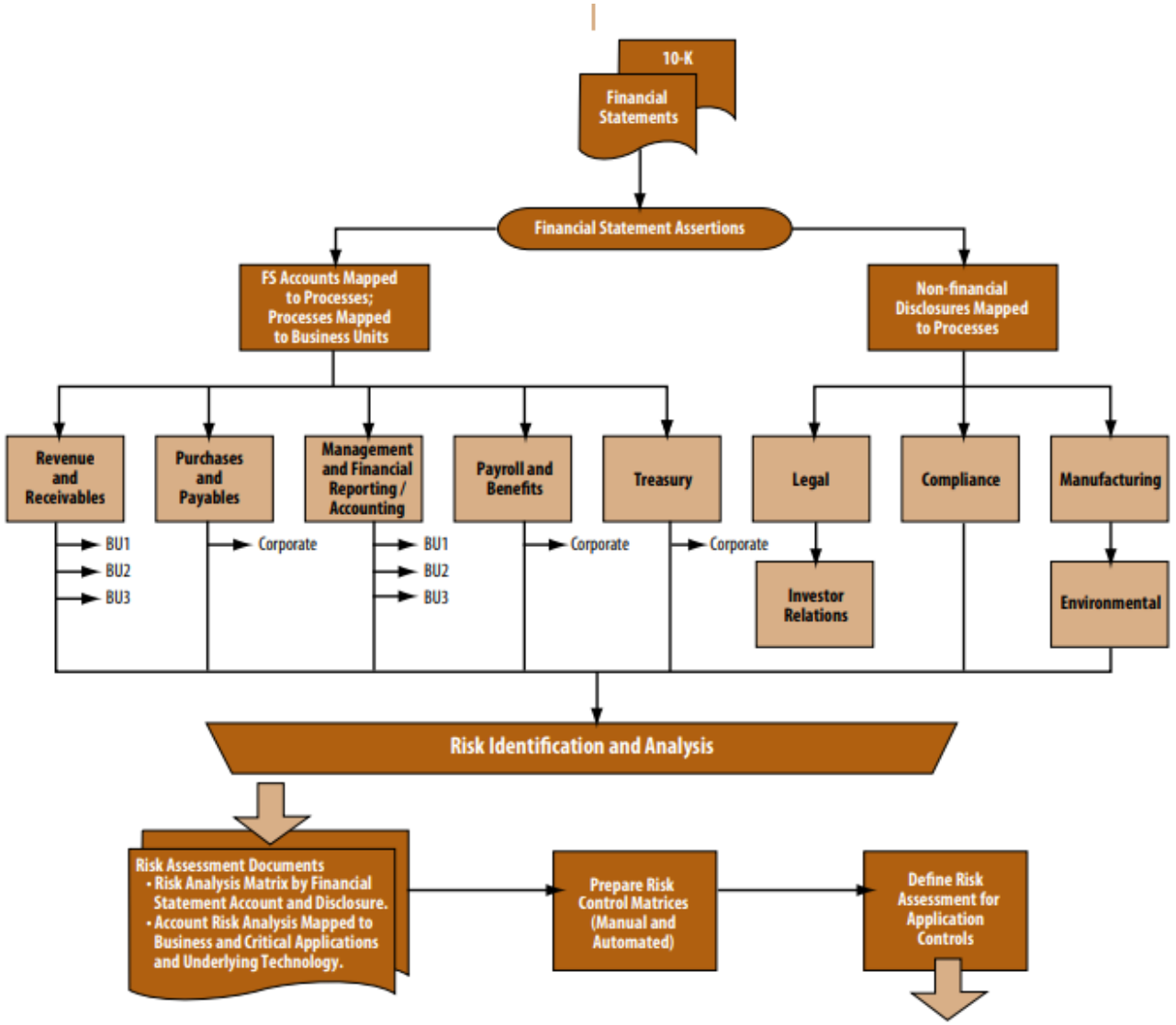

Structure of session
Why do we need risk management
Governance and risk management
COSO model
Risk assessment process
Risk categories
Risk management policy
Risk and control matrix
Risk appetite and risk tolerance
Risk reporting

Enterprise Risk Management (ERM) Approach

The structured ERM approach defines the key risks to business objectives across the organization and evaluates the level of management preparedness to clearly define opportunities to improve and/or monitor risks.



Process universe

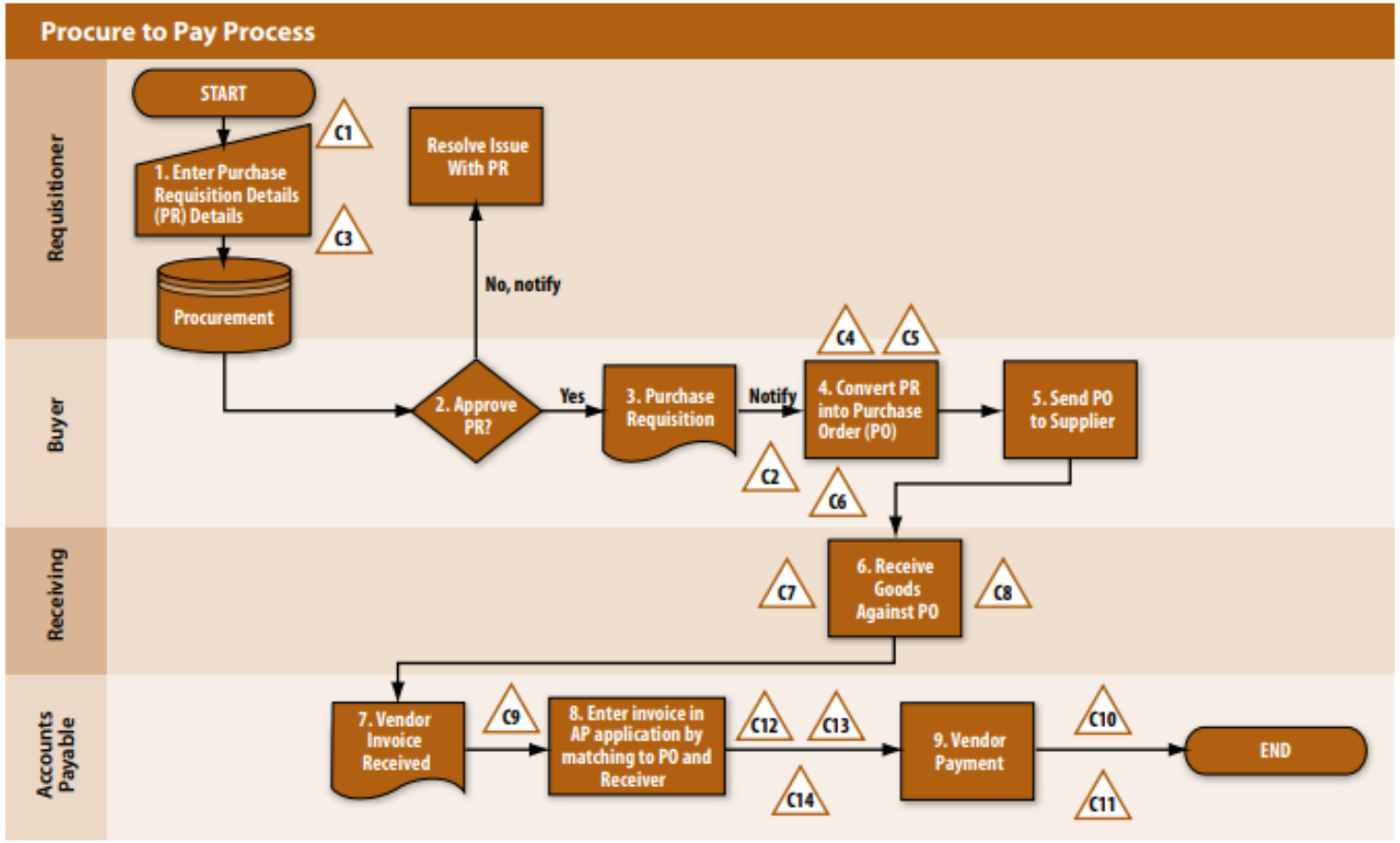


Mega Process (Level 1): Procure-to-Pay

Major Process (Level 2)	Subprocess (Level 3)	Activity (Level 4)
Procurement	Requisition processing	Create, change, and delete
	Purchase order processing	Create, change, delete, approval, and release
Receiving	Goods receipt processing	Create, change, and delete
	Goods return processing	Create, change, and delete
Accounts Payable	Vendor management	Create, change, and delete
	Invoice processing	Create, change, and delete
	Credit memo processing	Create, change, and delete
	Process payments	Create, change, and delete
	Void payments	Create, change, and delete


Structure of session
Why do we need risk management
Governance and risk management
COSO model
Risk assessment process
Risk categories
Risk management policy
Risk and control matrix
Risk appetite and risk tolerance
Risk reporting

Process overview flowchart



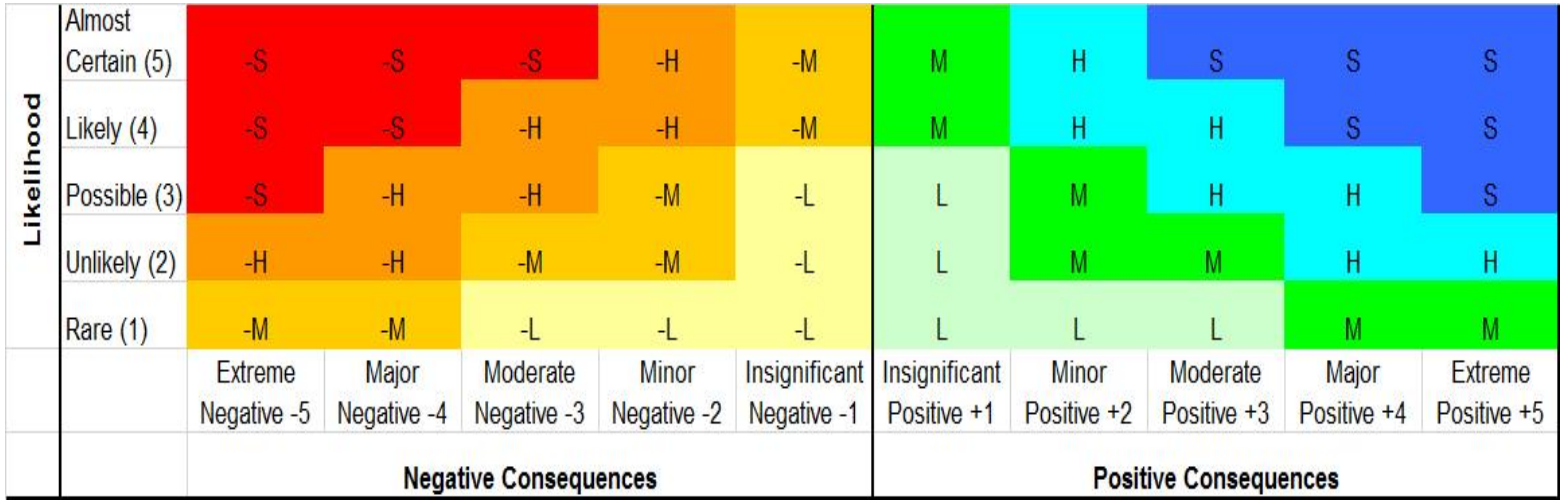
Risk and Control Matrix: Procure-to-Pay

	BUSINESS PROCESS & CONTROL OBJECTIVES	RISKS		CONTROL ACTIVITIES	COSO COMPONENTS					CONTROL ATTRIBUTES				CONTROL CLASSIFICATION						TESTING		
Number	Control Objectives	Risks	Impact/ Likelihood	Control Activities	CE	RA	CA	I/C	M	K (Y/N)	Man/Auto	Pre/Det	Frequency	Real	Recorded	Valued	Timely	Classified	Posted	Test Results	Operational Effectiveness (Y/N)	Notes

Risk management strategy

- Avoid
- Accept
- Transfer
- Mitigate

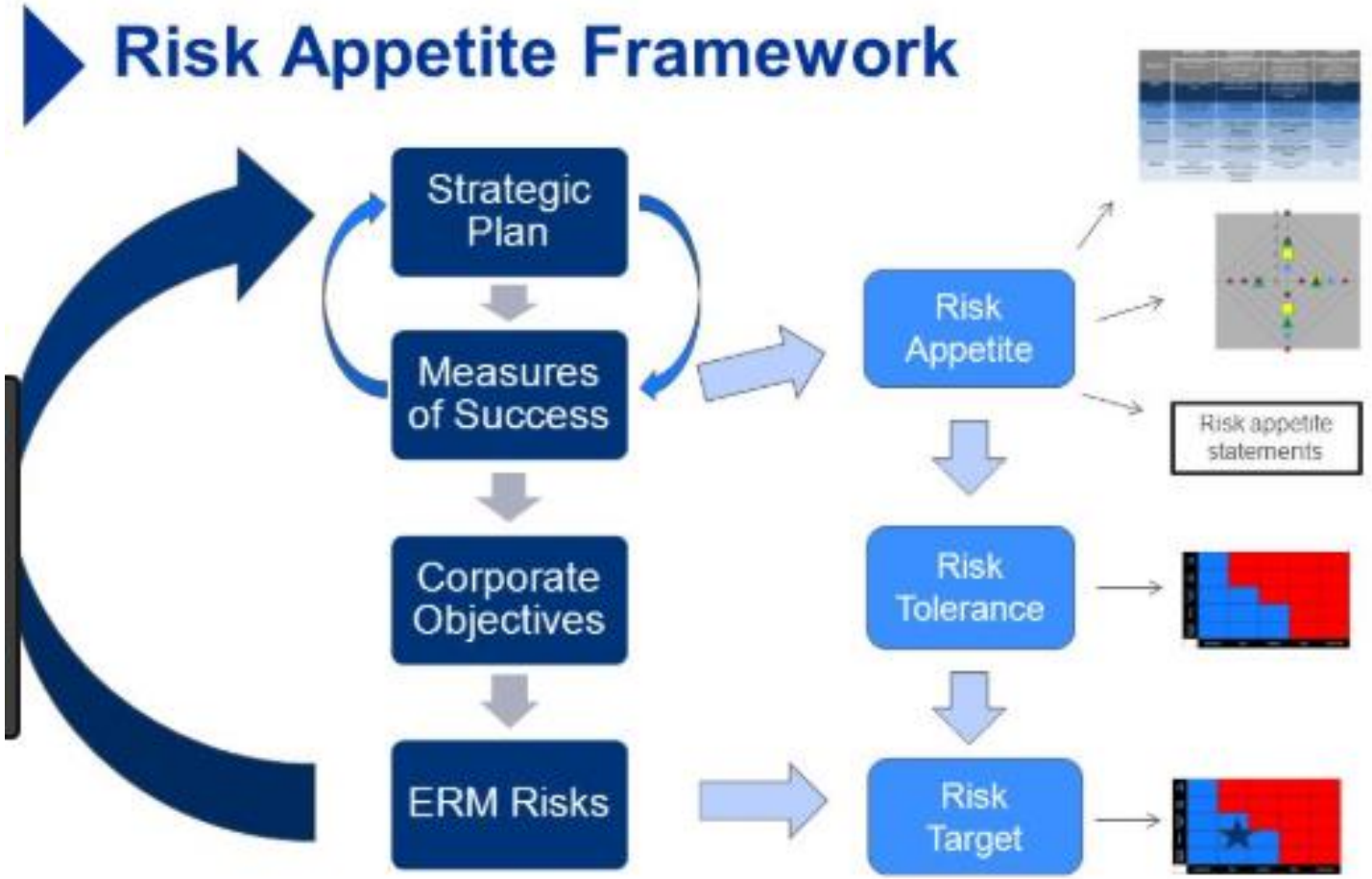
Take risk



Likelihood											
	Almost Certain (5)	-S	-S	-S	-H	-M	M	H	S	S	S
	Likely (4)	-S	-S	-H	-H	-M	M	H	H	S	S
	Possible (3)	-S	-H	-H	-M	-L	L	M	H	H	S
	Unlikely (2)	-H	-H	-M	-M	-L	L	M	M	H	H
	Rare (1)	-M	-M	-L	-L	-L	L	L	L	M	M
		Extreme Negative -5	Major Negative -4	Moderate Negative -3	Minor Negative -2	Insignificant Negative -1	Insignificant Positive +1	Minor Positive +2	Moderate Positive +3	Major Positive +4	Extreme Positive +5
		Negative Consequences					Positive Consequences				

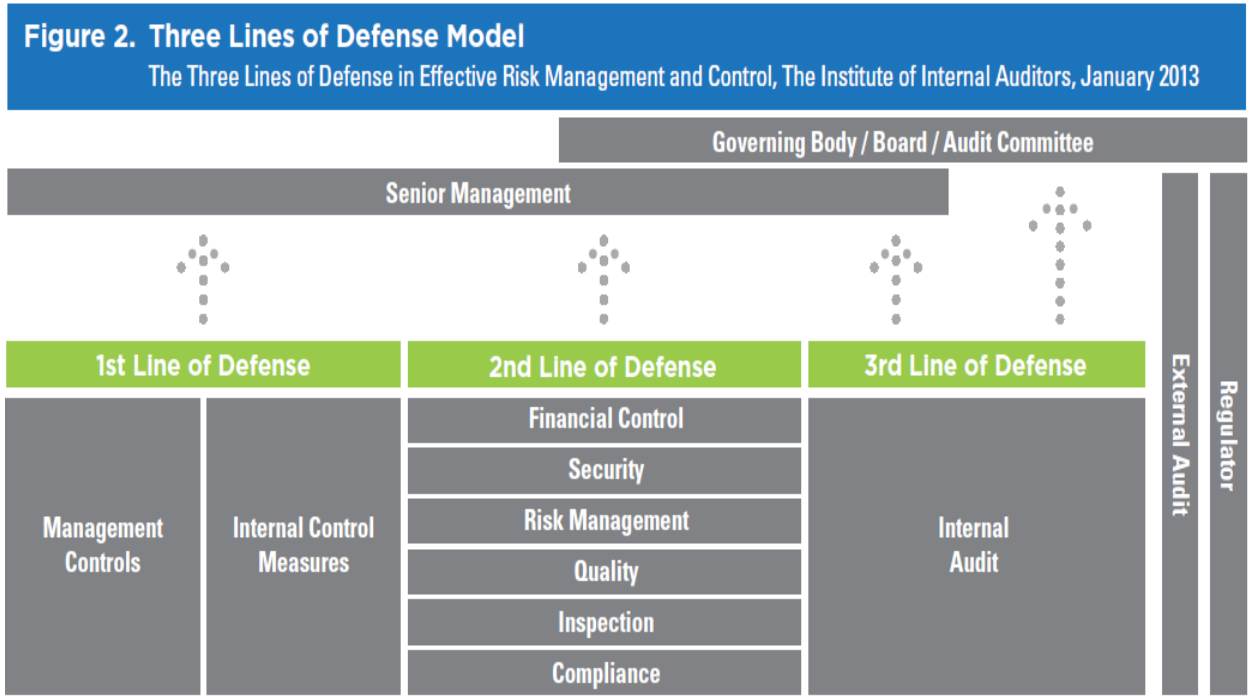

Structure of session
Why do we need risk management
Governance and risk management
COSO model
Risk assessment process
Risk categories
Risk management policy
Risk and control matrix
Risk appetite and risk tolerance
Risk reporting

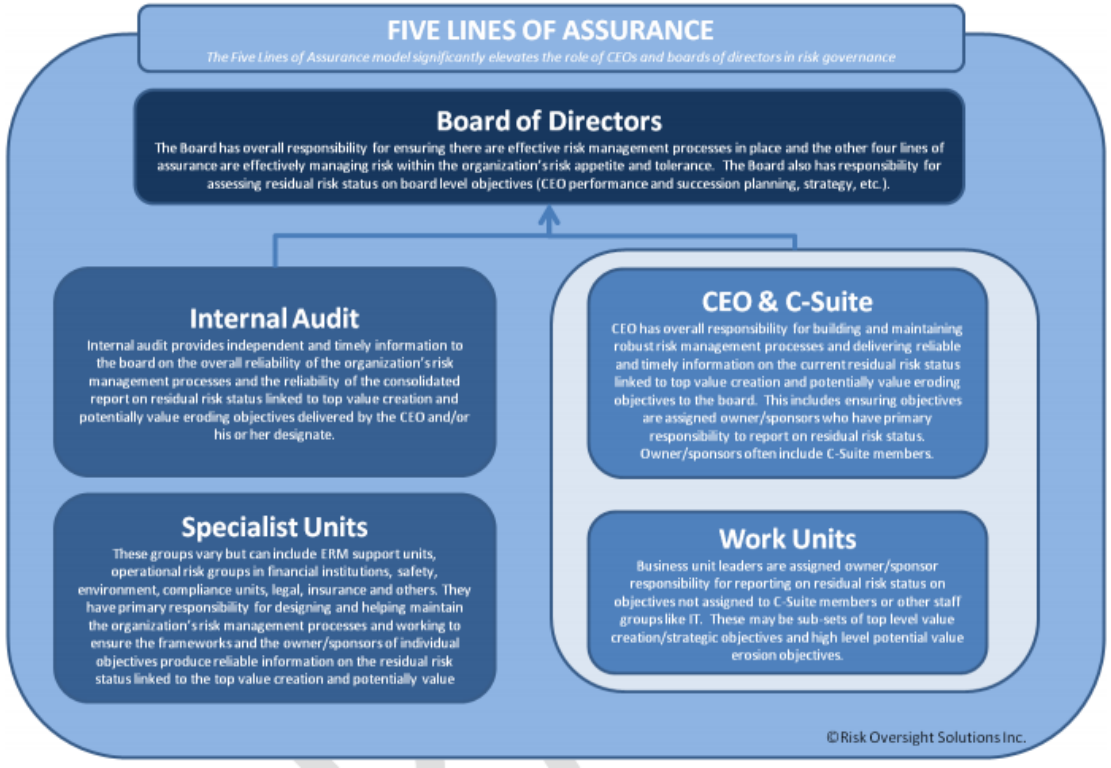
Residual risk versus risk appetite



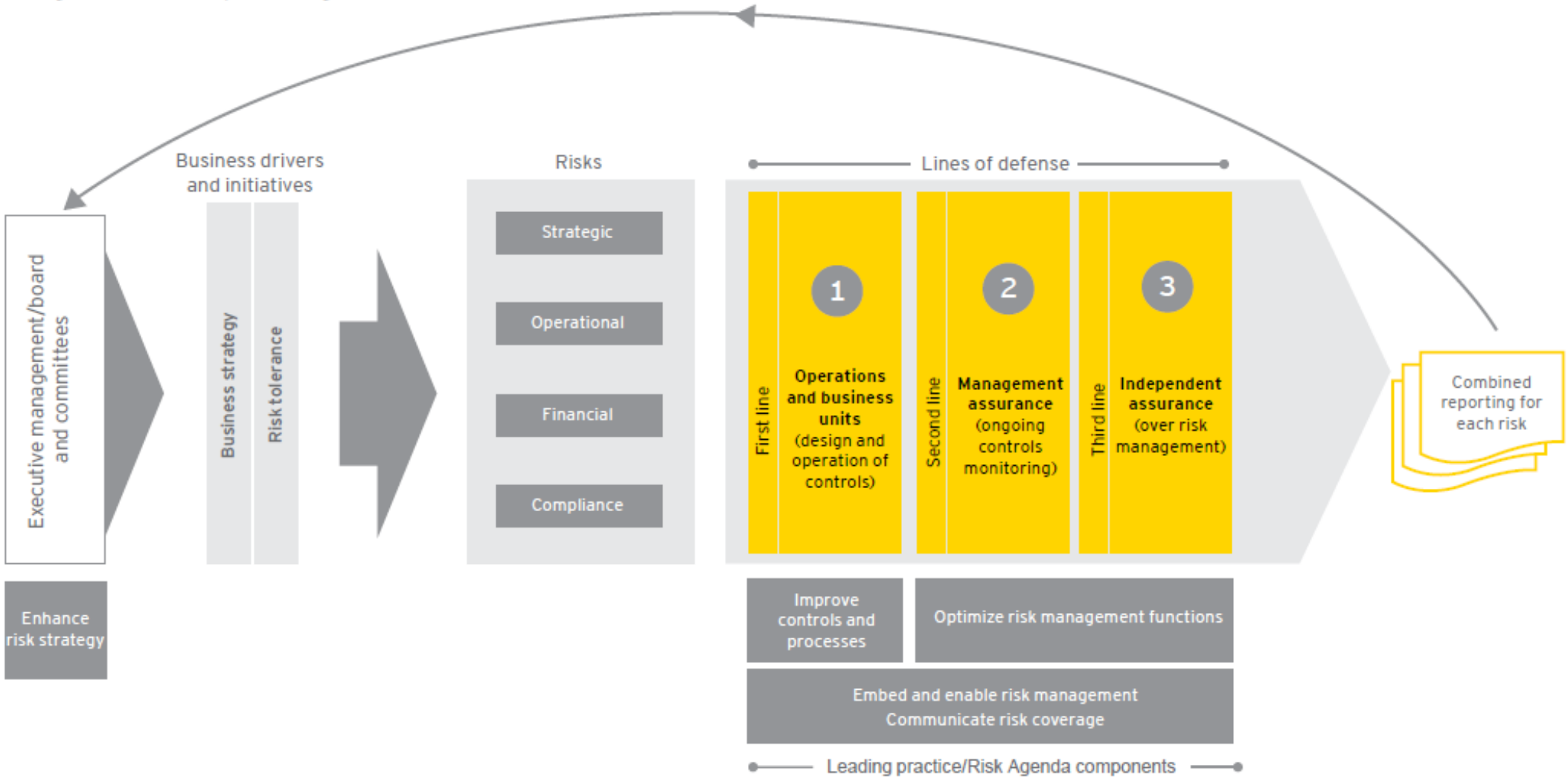

Structure of session
Why do we need risk management
Governance and risk management
COSO model
Risk assessment process
Risk categories
Risk management policy
Risk and control matrix
Risk appetite and risk tolerance
Risk reporting

Combined assurance





Integrated LOD (Lines of Defense) Model



Example: Risk Status Report