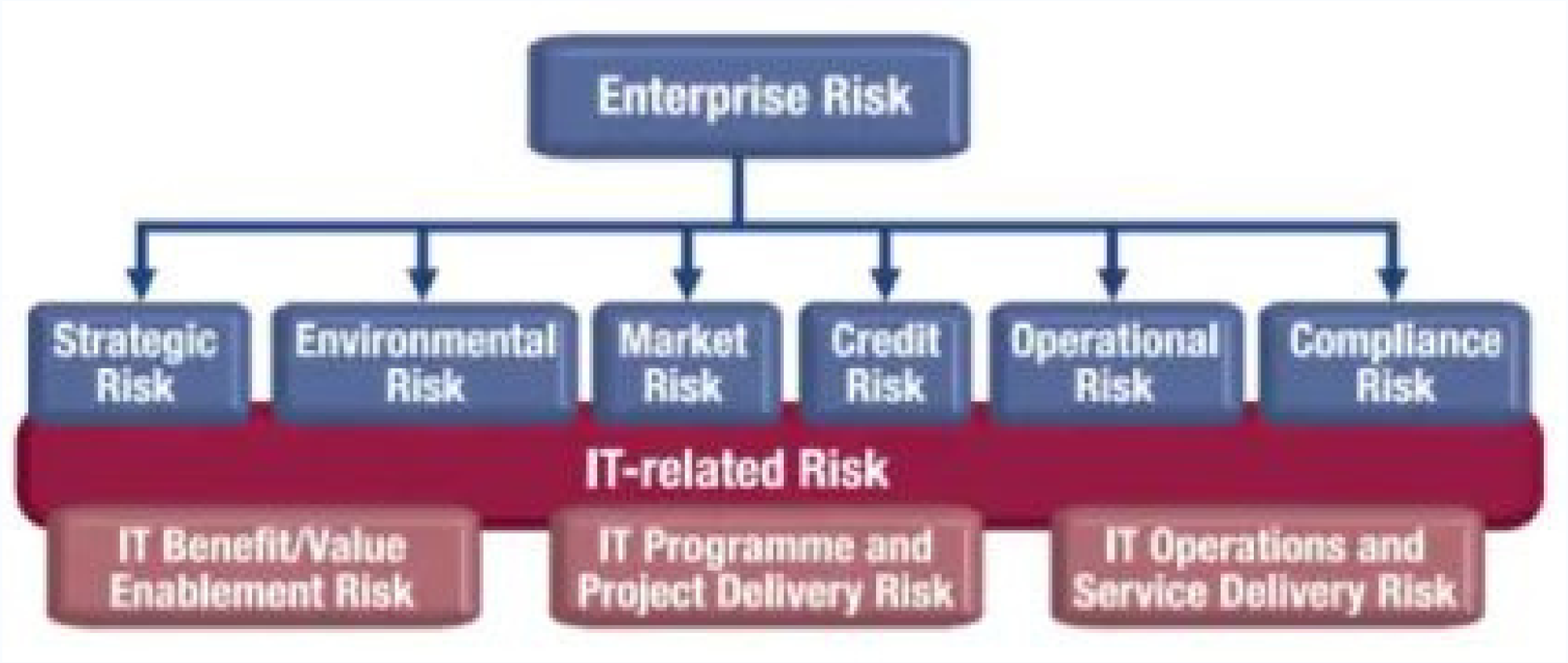
# COBIT

# WHY USE BEST PRACTICE/FRAMEWORK

- Better accountability and responsibility (ownership)
  - You get out of the blame game
- Better management
- Better benefits from IT investments
- Better compliance
- Better monitoring
- Easily compare yourself with others

- Everybody's doing it anyway
  - ITIL, ISO 27001/2, COSO ERM, PRINCE2, PMBOK, Six Sigma, TOGAF, etc.

# IT RELATED RISKS



# COBIT

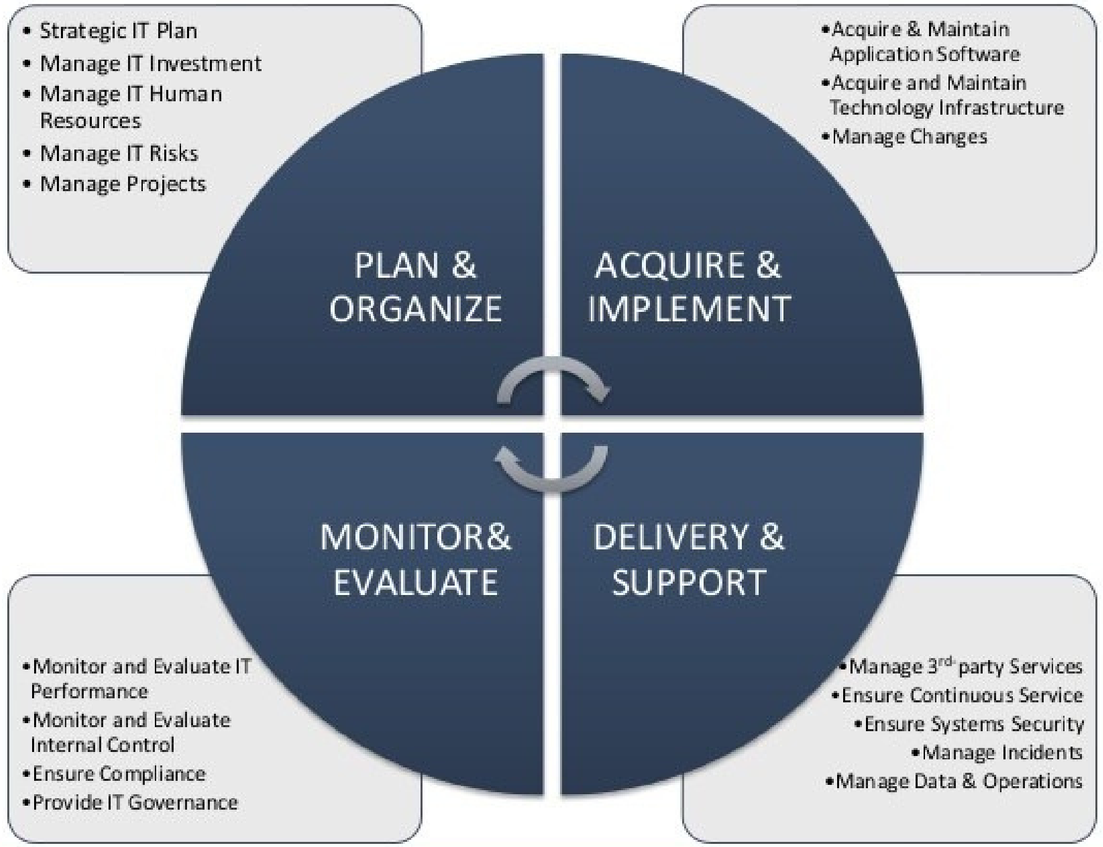
- A comprehensive IT governance and management framework
- Addresses every aspect of IT
- Ensures clear ownership and responsibilities
- A common language for all
- Improves IT efficiency and effectiveness
- Better management of IT investments
- Ensures compliance

- A complementary copy is available:
  - www.isaca.org/cobit

COBIT 5

# COBIT COVERAGE

## COBIT® coverage



# RISK IT

- Framework for effective management of IT risk
- Complements COBIT®
  - COBIT® provides a set of controls to mitigate IT risk
  - Risk IT provides a framework for enterprises to identify, govern and manage IT risk
- Enterprises who have adopted COBIT® can use Risk IT to enhance risk management
- Integrates the management of IT risk into the overall enterprise risk management (ERM) of the organization
- Helps management make well-informed decisions about the extent of the risk, the risk appetite and the risk tolerance of the enterprise
- Helps management understand how to respond to risk

- Available for ISACA members:
  - http://isaca.org/RiskIT

# RISK IT PRINCIPLES

- Always connects to business objectives
- Aligns the management of IT-related business risk with overall enterprise risk management (ERM) - if applicable
- Balances the costs and benefits of managing IT risk
- Promotes fair and open communication of IT risk
- Establishes the right tone from the top while defining and enforcing personal accountability for operating within acceptable and well-defined tolerance levels
- Is a continuous process and part of daily activities

# MANAGING & UNDERSTANDING IT RISK

- To prioritize and manage IT risk, management needs a clear understanding of the IT function and IT risk
  - Key stakeholders often do not have a full understanding
- IT risk is not just a technical issue
  - IT experts help to understand and manage aspects of IT risk
  - Business management is still the most important stakeholder
- Business managers determine what IT needs to do to support their business
  - They set the targets for IT
  - They are accountable for managing the associated risks

# RISK IT PROCESS MODEL

1. Define a risk universe and scoping risk management
2. Risk appetite and risk tolerance
3. Risk awareness, communication and reporting: includes key risk indicators, risk profiles, risk aggregation and risk culture
4. Express and describe risk: guidance on business context, frequency, impact, COBIT business goals, risk maps, risk registers
5. Risk scenarios: includes capability risk factors and environmental risk factors
6. Risk response and prioritization
7. A risk analysis workflow: "swim lane" flow chart, including role context
8. IT risk mitigation using COBIT and Val IT

# RISK IT PUBLICATIONS

- Risk IT Framework
  - A set of governance practices for risk management
  - An end-to-end process framework for successful IT risk management
  - A generic list of common, potentially adverse, IT-related risk scenarios
  - Tools and techniques to understand concrete risks to business operations

- Risk IT Practitioner Guide
  - **Support document** for the Risk IT framework
  - Provides examples of possible techniques to address IT-related risk issues
  - Building scenarios, based on a set of generic IT risk scenarios
  - Building risk maps, techniques to describe scenario impact and frequency
  - Building impact criteria with business relevance
  - Defining KRIs (Key Risk Indicators)

# RACI CHART

## RACI charts – IT risk example

| Key activities / Roles | Board | CEO | CRO | CIO | CFO | Enterprise Risk Committee | Business Management | Business Process Owner | Risk Control Functions | HR | Compliance and Audit |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Define IT risk analysis scope | | I | R | C | I | C | A | R | C | | C |
| Estimate IT risk | | I | R | C | C | I | A/R | R | R | | C |
| Identify risk response options | | | C | C | C | R | A | R | R | | I |
| Perform a peer review of IT analysis | | | A/R | | | | I | | I | | I |
| Perform enterprise IT risk assessment | I | A | R | R | C | I | R | C | R | C | C |
| Propose IT risk tolerance thresholds | I | I | C | R | C | I | A | C | C | | C |
| Approve IT risk tolerance | A | C | C | C | C | R | C | C | C | C | C |
| Assign IT risk policy | C | A | R | R | R | C | R | R | R | R | C |
| Promote IT risk-aware culture | A | R | R | R | R | R | R | R | R | R | R |
| Encourage effective communication of IT risk | R | R | R | R | R | R | A | R | R | R | R |

A **RACI chart** identifies who is **Responsible**, **Accountable**, **Consulted** and/or **Informed**

# COBIT
# RISK GOVERNANCE

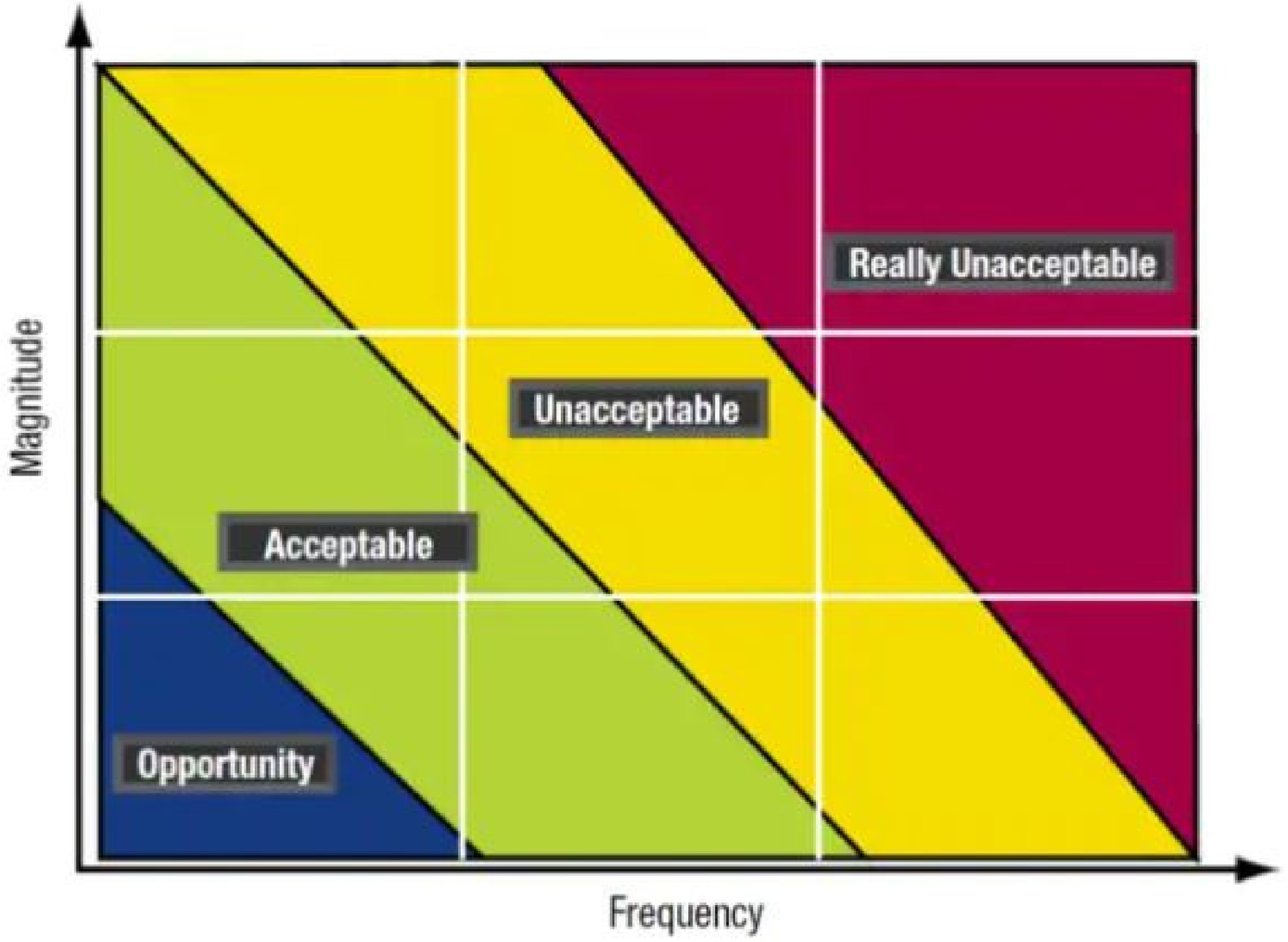
# Risk governance, evaluation and response

- Risk Governance
  - Establish and Maintain a Common Risk View
  - Integrate with Enterprise Risk Management (ERM)
  - Make Risk-aware Business Decisions
- Risk Evaluation
  - Collect Data
  - Analyze Risk
  - Maintain Risk Profile
- Risk Response
  - Articulate Risk
  - Manage Risk
  - React to Events

# RISK APPETIT & RISK TOLERANT

- Risk Appetite: the amount of risk an entity is prepared to accept when trying to achieve its objectives
  - Defining factors:
    - The enterprise's objective capacity to absorb loss (e.g., financial loss, reputation damage)
    - The (management) culture or predisposition towards risk taking - cautious or aggressive (i.e. what is the amount of loss the enterprise wants to accept to pursue a return?)
- Risk Tolerance: the tolerable deviation from the level set by the risk appetite and business objectives
  - e.g., standards require projects to be completed within estimated budgets and time, but overruns of 10 percent of budget or 20 percent of time are tolerated

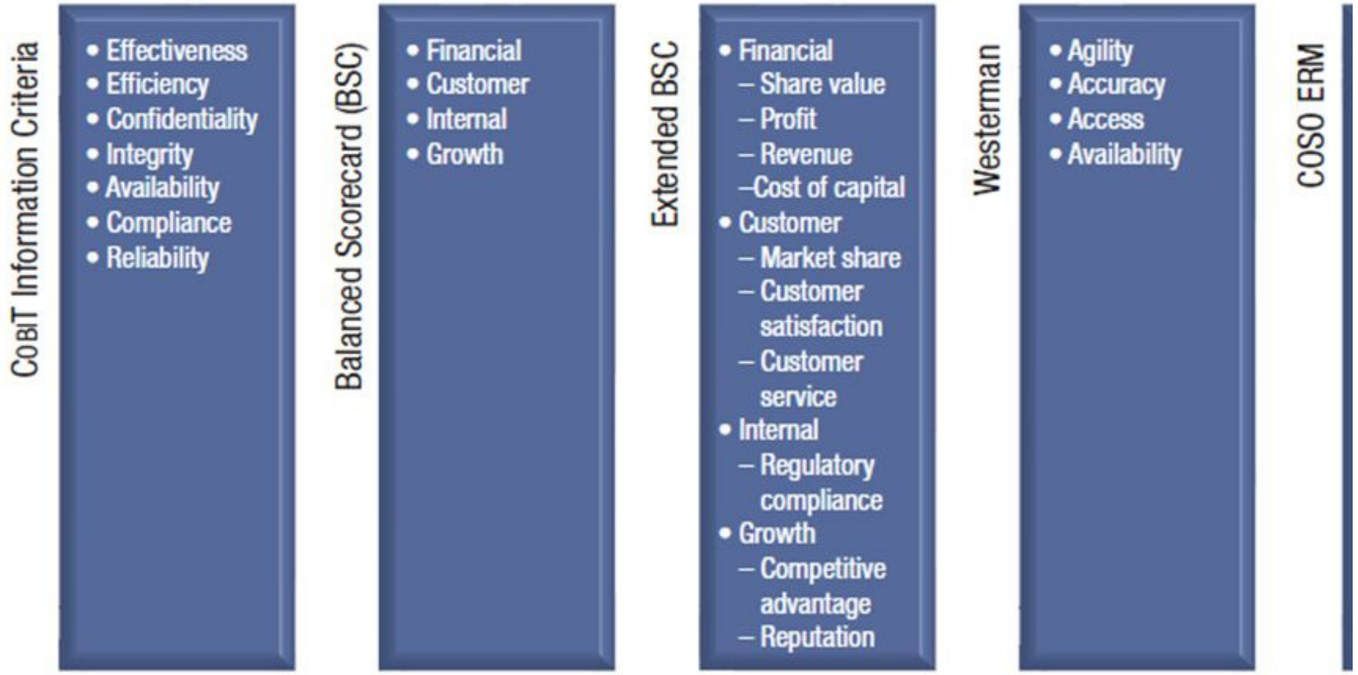
# RISK MAP


Really Unacceptable
Unacceptable
Acceptable
Opportunity
Magnitude
Frequency

# ELEMENT OF RISK CULTURE

# EXPRESSING IT RISK IN BUSINESS TERM

Figure 12—Expressing IT Risk in Business Terms



# IT RISK SECARIO COMPONENT

# RISK RESPONSE

- Identify Key Risk Indicators based on:
  - Impact
  - Effort to implement, measure and report
  - Reliability
  - Sensitivity
- Decide on best response to risk
  - Avoidance
  - Reduction/Mitigation
  - Sharing/Transfer
  - Acceptance