Risk IT – Bridging the Gap

Bob Fabian
www.fabian.ca
Toronto 2010.03.30

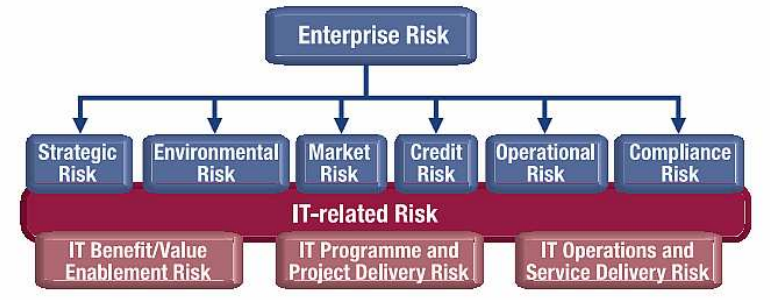
My Background

- Involved in computing 50+ years
- Mixed bag:
  - Academic, consultant, manager
- Critical Change ~ 2000
  - Practical Best Practices
- Risk Best Practice
  - IT Professional Responsibility
  - CIPS Risk Guideline – lead author
  - ITGI Risk IT – one of the reviewers

Plan for Session

- Who's doing it?
- International Risk Management
- IT Professional Risk Management
- The ITGI Risk Context
- The Risk IT Content
- Open: Bridging the Gap

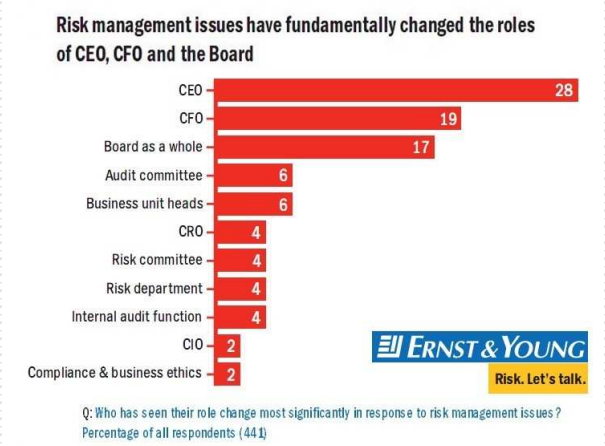
ITGI View



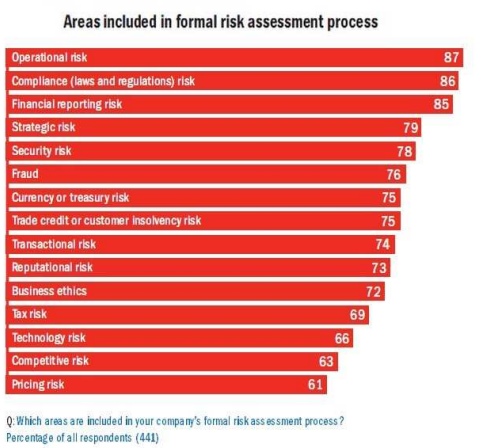
Who's Doing It?

- Demand on Boards / Sr. Management
  - Lip service guaranteed
  - Risk Management Best Practice
- Prudent Professional Responsibility
  - Makes practical project sense
  - Part of legal duty of care
- IT Management in the Middle
- Still, … Audit needs to be ready

Risk Management Changes



Risk Management Concerns



Senior Management

- Risk not part of purchasing
  - No risk with purchase of a ton of sand
  - No risk with purchase of new system
- No easy way to include system risk
  - No objective system risk rating service
- Orders come after Board decisions
  - IT rarely invited to Board discussions

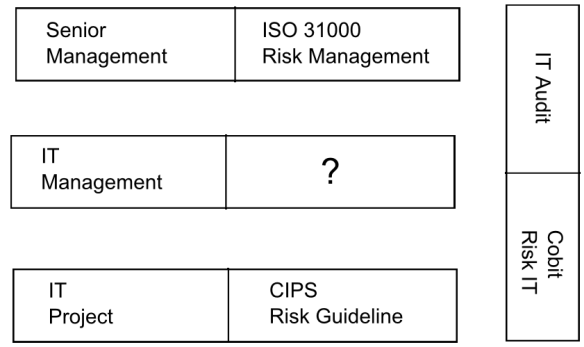
IT Project Management

- Risk management seen as important
  - Part of drive to agile, spiral
- Professional importance of risk management
  - Prudent for project manager
  - Required from a professional
- Growing "traction"

IT Management

- "Man-in-the-Middle"
  - Orders come down from on high
  - Plans come up from below
- Coincidence of risk – happy accident
- Cobit Risk IT provides framework
  - Need empowerment to employ

IT Risk Universe



Clarification

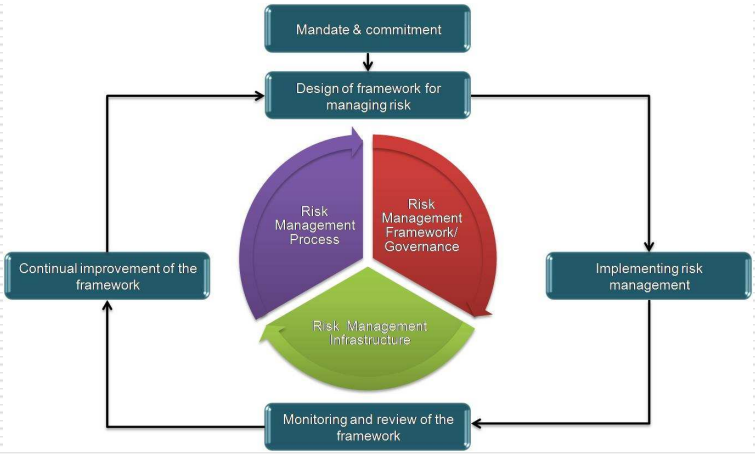
- ISO 31000 *the* International risk management standard
  - Accepted by CSA
- CIPS Risk Management Guideline is only one possible approach
  - Software Engineering Institute
  - Project Management Institute
  - Etc.

Requisite Variety

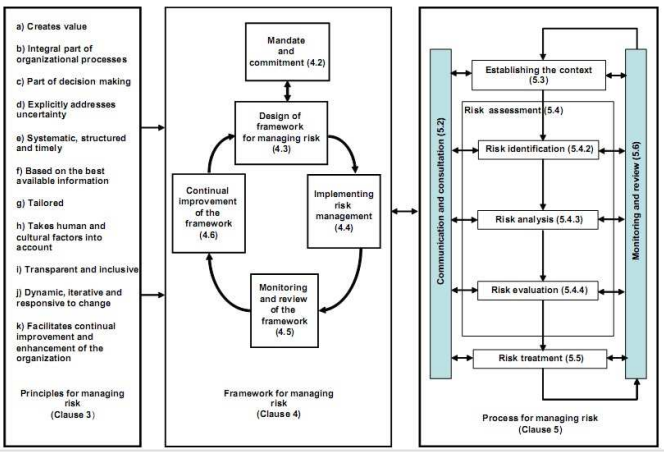
- Every Good Regulator of a system must be a model of that system.
  - Conant & Ashby
  - Interpretation: The regulator must have a model that's at least as complex as the model governing the system.
  - Implication: IT Audit needs a risk model at least as complex as that used by IT Management.
- Risk IT important for IT Audit!

The International Standard

ISO 31000 Universe



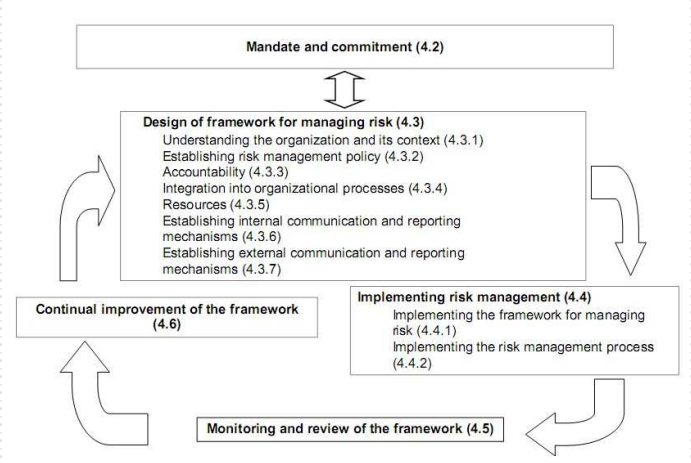
ISO 31000 Overview



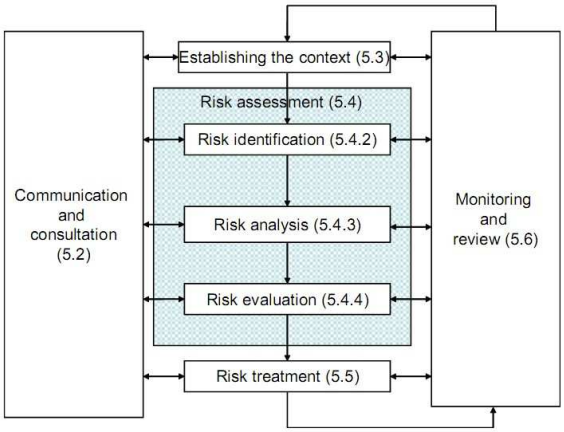
Managing Risk Principles

- Creates and protects value
- Integral part of organizational process
- Part of decision making
- Explicitly addresses uncertainty
- Systematic, structured and timely
- Based on the best available information
- Tailored
- Takes human and cultural factor into account
- Transparent and inclusive
- Dynamic, interactive and responsive to change
- Facilitates continual improvement of the organization

Activity Breakdown



Risk Management Process



View of ISO 31000

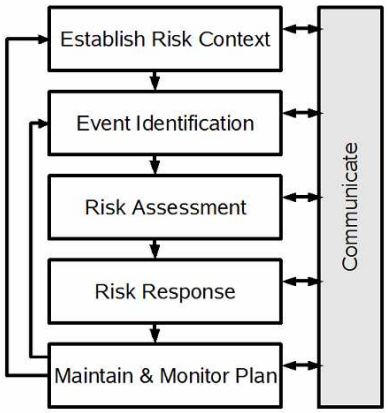
- Framework is valid and valuable
- Has been accepted internationally
  - and in Canada too
- But it's only a framework
  - Tailoring (instantiation) essential
- Useful starting point

IT Professional Risk Guideline

Risk Management Practice Guideline

February 2007

CIPS Risk Management Flow



Communicate

- Important to tell people about risks
  - Above
  - Below
  - Besides
  - Following
- It's a *professional* responsibility
- It makes *business* sense

Risk Context

- What practices are to be followed?
- Event assessment
  - Who has a voice, how much detail?
- Outcome gap assessment
  - Who has a voice, how much detail?
- Risk response plan
  - Who has a voice, how much detail?

Event Identification

Four broad approaches

1. Judgement – individuals/groups use their best judgement
2. Scenarios – examine qualitatively different alternatives
3. Models – formally model the activities under review
4. Check Lists – use check lists or taxonomies of possible risks

Risk Assessment

- Assess *likelihood* and *impact* of all identified risk events
- Use quantitative *and* qualitative methods
- Determine *inherent* and *residual* risks
  - Effort to mitigate, then ...
  - How much risk remains?

Risk Response

- Four broad approaches:
  - Tolerate – live with the consequences, e.g. self insure
  - Transfer – find insurance/contractor to assume the risk
  - Reduce – change plans to reduce probability or impact
  - Eliminate – don't engage in activities with unacceptably severity

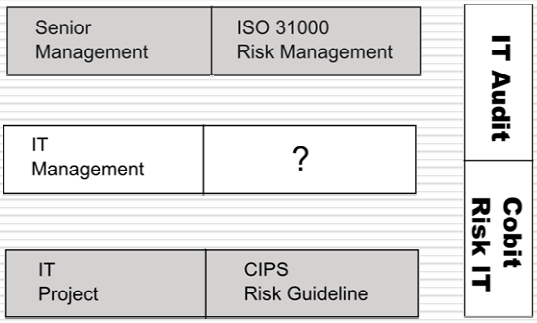
Maintain & Monitor Plan

- Control activities to implement necessary risk responses
  - Costs, benefits, responsibilities
- Ensure committed actions are really owned
- Active monitor for risk events
- Monitor execution of plans
- Review/revise with stakeholders

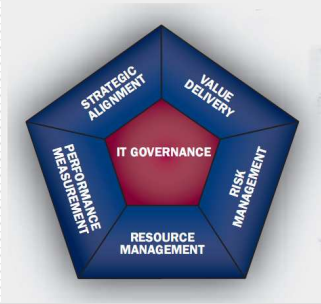
It's More Than Projects

- Acquisition
  - Buy the wrong thing (bad spec/selection)
  - Thing evolves incorrectly (wrong dynamic)
- Operations
  - Not adequately managing operations
  - Successful external attack on system
- Development
  - Failure to meet the project's goals
  - Failure to address *real* opportunities

IT Audit Risk World

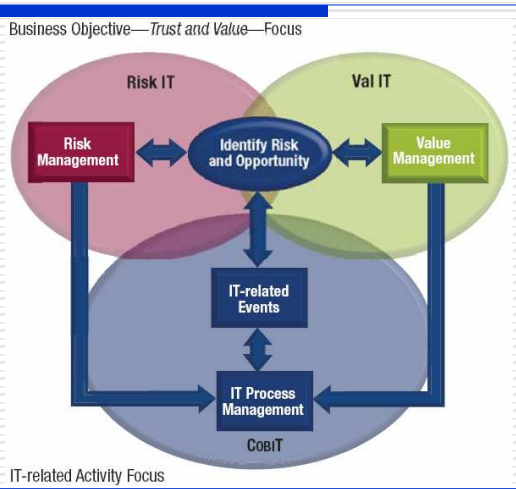


COBIT View



- Strategic alignment
- **Value delivery**
- Resource management
- **Risk management**
- Performance management

Big 3 ITGI Frameworks



CobiT Risk Breakdown

Assess and manage IT risks

that satisfies the business requirement for IT of

analysing and communicating IT risks and their potential impact on business processes and goals

by focusing on

development of a risk management framework that is integrated in business and operational risk management frameworks, risk assessment, risk mitigation and communication of residual risk

is achieved by

- Ensuring that risk management is fully embedded in management processes, internally and externally, and consistently applied
- Performing risk assessments
- Recommending and communicating risk remedial action plans

and is measured by

- Percent of critical IT objectives covered by risk assessment
- Percent of identified critical IT risks with action plans developed
- Percent of risk management action plans approved for implementation

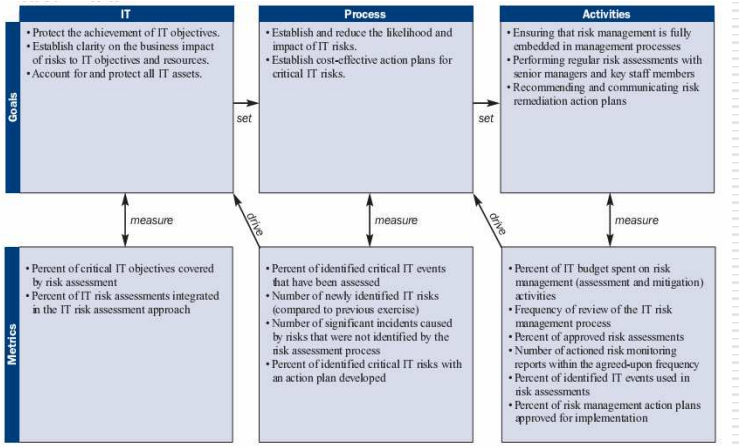
COBIT: Risk Input & Output

PO9 Assess and Manage IT Risks

From	Inputs
PO1	Strategic and tactical IT plans, IT service portfolio
PO10	Project risk management plan
DS2	Supplier risks
DS4	Contingency test results
DS5	Security threats and vulnerabilities
ME1	Historical risk trends and events
ME4	Enterprise appetite for IT risks

Outputs	To						
Risk assessment	PO1	DS4	DS5	DS12	ME4		
Risk reporting	ME4						
IT-related risk management guidelines	PO6						
IT-related risk remedial action plans	PO4	AI6					

Goals & Metrics



COBIT: Risk RACI Chart

RACI Chart **Functions**

Activities	CEO	CFO	Business Executive	CIO	Business Senior Management	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Determine risk management alignment (e.g., assess risk).	A	R/A	C	C	R/A	I					I
Understand relevant strategic business objectives.		C	C	R/A	C	C					I
Understand relevant business process objectives.				C	C	R/A					I
Identify internal IT objectives and establish risk context.					R/A		C	C	C		I
Identify events associated with objectives [some events are business-oriented (business is A); some are IT-oriented (IT is A, business is C)].	I			A/C	A	R	R	R	R		C
Assess risk associated with events.				A/C	A	R	R	R	R		C
Evaluate risk responses.	I	I	A	A/C	A	R	R	R	R		C
Prioritise and plan control activities.	C	C	A	A	R	R	C	C	C		C
Approve and ensure funding for risk action plans.		A	A		R	I	I	I	I		I
Maintain and monitor a risk action plan.	A	C	I	R	R	C	C	C	C	C	R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

CobiT Risk Management Levels

1 Initial/Ad Hoc
2 Repeatable but Intuitive
3 Defined Process
4 Managed and Measurable
5 Optimised

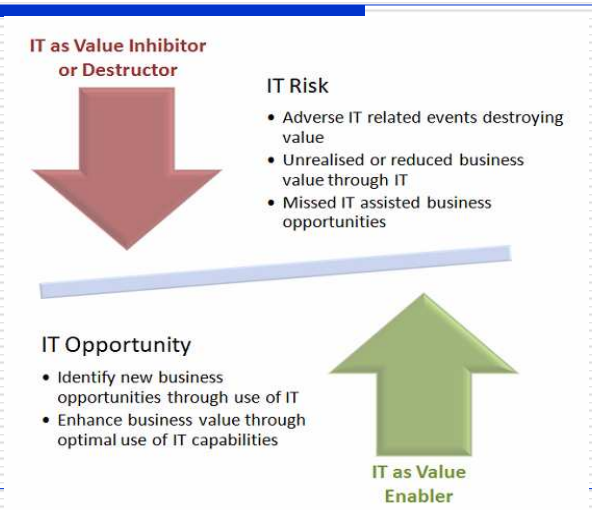
3: Defined Process

- "An organisationwide risk management policy defines when and how to conduct risk assessments. Risk management follows a defined process that is documented. Risk management training is available to all staff. Decisions to follow the risk management process and to receive training are left to the individual's discretion. The methodology for the assessment of risk is convincing and sound and ensures that key risks to the business are identified. A process to mitigate key risks is usually instituted once the risks are identified. Job descriptions consider risk management responsibilities."

Time Line

- It started with COBIT
  - Now in version 4.1
- Then Val IT was added
  - Focus on program benefit
  - Now in version 2.0
- Risk IT has been released
  - Timely
  - Completes the picture

Risk / Value Balance



Now available …

Risk IT Definition

- **IT risk** is business risk -- specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption COBIT of IT within an enterprise. It consists of IT-related events that could IT-related Activity Focus potentially impact the business. It can occur with both uncertain frequency and magnitude, and it creates challenges in meeting strategic goals and objectives. IT risk can be categorized in different ways:
  - **IT benefit/value enablement risk**, associated with (missed) opportunities to use technology t improve efficiency or effectiveness of business processes, or as an enabler for new business initiatives
  - **IT programme and project delivery risk**, associated with the contribution of IT to new or improved business solutions, usually in the form of projects and programmes. This ties to investment portfolio management (as in Val IT).
  - **IT operations and service deliver risk**, associated with all aspects of the performance of IT systems and services, which can bring destruction or reduction of value to the enterprise
- IT risk always exists, whether or not it is detected or recognized by an organization.

Responsibilities & Accountabilities 1

Role Definitions		Risk Governance			Risk Evaluation			Risk Response		
Role	Suggested Definition	Common Risk View	Integrate With ERM	Risk-aware Decisions	Collect Data	Analyse Risk	Maintain Risk Profile	Articulate Risk	Manage Risk	React to Events
Board	The most senior executives and/or non-executives of the enterprise who are accountable for the governance of the enterprise and have overall control of its resources	■	■							
Chief executive officer (CEO)	The highest-ranking officer who is in charge of the total management of the enterprise	■	■						■	
Chief risk officer (CRO)	The individual who oversees all aspects of risk management across the enterprise. An IT risk officer function may be established to oversee IT-related risk.	■	■	■	■	■	■	■	■	■
Chief information officer (CIO)	The most senior official of the enterprise who is accountable for IT advocacy; aligning IT and business strategies; and planning, resourcing and managing the delivery of IT services and information and the deployment of associated human resources. The CIO typically chairs the governance council that manages the portfolio.	■	■	■	■	■	■	■	■	■
CFO	The most senior official of the enterprise who is accountable for financial planning, record keeping, investor relations and financial risks	■								
Enterprise risk committee	The executives who are accountable for the enterprise-level collaboration and consensus required to support enterprise risk management (ERM) activities and decisions. An IT risk council may be established to consider IT risk in more detail and advise the enterprise risk committee.	■		■		■		■		

Responsibilities & Accountabilities 2

Role Definitions		Risk Governance			Risk Evaluation			Risk Response		
Role	Suggested Definition	Common Risk View	Integrate With ERM	Risk-aware Decisions	Collect Data	Analyse Risk	Maintain Risk Profile	Articulate Risk	Manage Risk	React to Events
Business management	Business individuals with roles relating to managing a programme(s)	■	■	■		■	■	■	■	■
Business process owner	The individual responsible for identifying process requirements, approving process design and managing process performance. In general, a business process owner must be at an appropriately high level in the enterprise and have authority to commit resources to process-specific risk management activities.	■	■	■	■	■	■	■	■	■
Risk control functions	The functions in the enterprise responsible for managing certain risk focus areas (e.g., chief information security officer, business continuity plan/disaster recovery, supply chain, project management office)	■	■	■	■	■	■	■	■	■
Human resources (HR)	The most senior official of an enterprise who is accountable for planning and policies with respect to all human resources in that enterprise	■								
Compliance and audit	The function(s) in the enterprise responsible for compliance and audit	■								■

Legend of the table:
- Blue cell—The role carries responsibility and/or partial accountability for the process.
- Red cell—The role carries main accountability for this process. Only one role can be the main one accountable for a given process.

Risk IT Principles

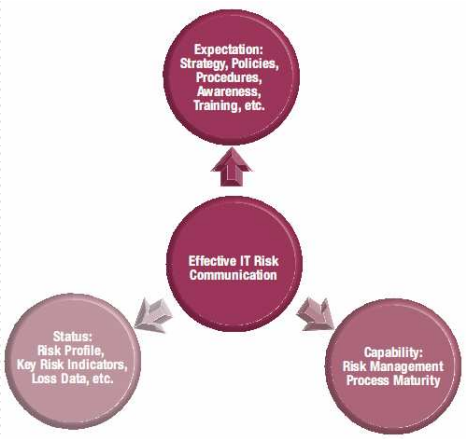
- Effective enterprise governance of IT risk always connects to business objectives
- Effective enterprise governance of IT risk aligns the management of IT-related business risk with overall enterprise risk management
- Effective enterprise governance of IT risk balances the costs and benefits of managing risk
- Effective management of IT risk promotes fair and open communication

Risk IT Principles II

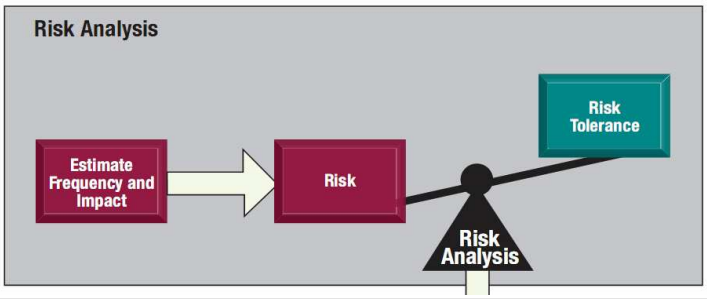
- Effective management of IT risk is a continuous process and part of daily activities
- Attention is paid to consistent risk assessment methods, roles and responsibilities, tools, techniques, and criteria across the enterprise
- Risk management practices are appropriately prioritised and embedded in enterprise decision-making processes
- Risk management practices are straightforward and easy to use, and contain practices to detect threat and potential risk, as well as prevent and mitigate it

Risk IT Overview

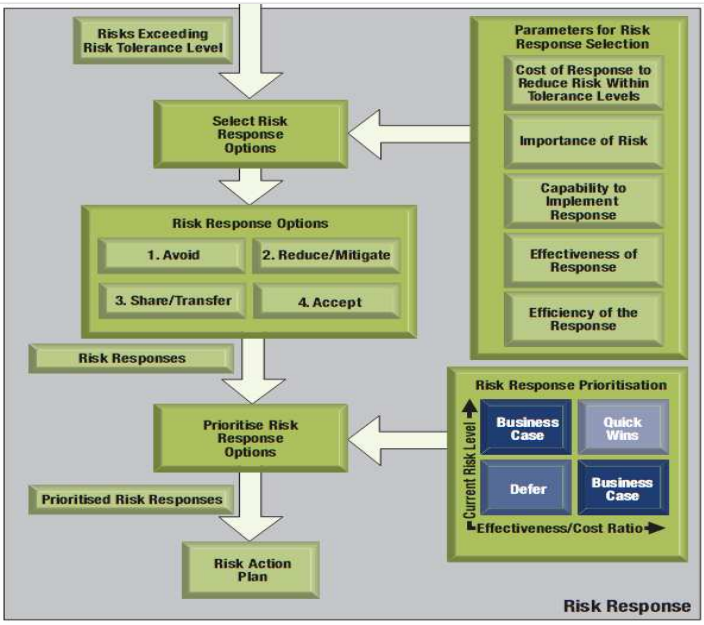
Risk Communication



Risk Analysis



Risk Response



Risk IT Domains

- Domain—Risk Governance (RG)
  - RG1 Establish and Maintain a Common Risk View
  - RG2 Integrate With Enterprise Risk Management (ERM)
  - RG3 Make Risk-aware Business Decisions
- Domain—Risk Evaluation (RE)
  - RE1 Collect Data
  - RE2 Analyse Risk
  - RE3 Maintain Risk Profile
- Domain—Risk Response (RR)
  - RR1 Articulate Risk
  - RR2 Manage Risk
  - RR3 React to Events

Risk Governance

- Domain Goal:
  - Ensure that IT risk management practices are embedded in the enterprise, enabling it to secure optimal risk adjusted return.
- Domain Metrics:
  - The degree to which the strategic use of IT in leveraging enterprise resources reduces overall enterprise risk.
  - Percentage of staff trained in critical risk management techniques (e.g., standard risk analysis techniques, crisis management, project management, skills of people (audit, etc.) to detect when something IT related is amiss)

RG1: Common Risk View

- Process Goal:
  - Ensure that risk management activities align with the organization's objective capacity for IT-related loss and leadership's subjective tolerance.
- Key Activities:
  - RG1.1 Develop an enterprise-specific IT risk management framework
  - RG1.2 Develop IT risk management methods
  - RG1.3 Perform an enterprisewide IT risk assessment
  - RG1.4 Propose IT risk tolerance thresholds
  - RG1.5 Approve IT risk tolerance
  - RG1.6 Align policy and standards statements with IT risk tolerance
  - RG1.7 Promote an IT risk aware culture
  - RG1.8 Promote effective communication of IT risk

RG1.1 Develop an enterprise-specific IT risk management framework

From	Inputs
RG1.3, COBIT ME4	Enterprise appetite for IT risk
RG2.3	IT risk management scope
RG2.3	Enterprise integrated risk reporting requirements
RG2.4	Updates to IT risk management framework
COBIT PO9	IT-related risk management guidelines
*	Enterprise risk management framework

To	Outputs
RG1.2, RG1.3, RG1.8, RE2.1	IT risk management framework

RG1.2 Develop IT risk management methods

From	Inputs
RG1.1	IT risk management framework
RG2.3	IT risk management scope
RG2.4	Updates to IT risk management methods
RG2.4	Updates to IT risk management process monitoring methods
RR3.4	Process improvements
COBIT PO9	IT-related risk management guidelines
*	Enterprise risk management framework

To	Outputs
RG1.3, RG1.4, RG1.6, RG2.4, RG3.1, RE2.1, RE2.2, RE3.2	IT risk management methods
RG2.4, RR3.4	IT risk management process monitoring methods

RG 1.3 Perform an enterprisewide IT risk assessment

From	Inputs
RG1.1	IT risk management framework
RG1.3	IT risk management methods
RG1.8, RR3.4	Request for enterprise-wide IT risk assessment
RG2.3	Enterprise risk elements to be included in IT risk assessments
RE1.4, RE1.5	Risk factors
RE3.3	IT capability mappings
Val IT PM1	IT strategy and goals feedback
Val IT IM7	Service portfolios
COBIT PO1	IT service portfolio, strategic IT plan, tactical IT plan
COBIT ME3	Report on compliance of IT activities with external legal and regulatory requirements
COBIT ME4	Enterprise strategic direction for IT
*	Enterprise strategy, objectives and goals

To	Outputs
RG1.1, RG1.4, RG1.5, RG2.3, COBIT PO9	Enterprise appetite for IT risk
RG1.4, RG1.5, RG2.3, RG3.3, RE3.1, RE3.4, COBIT PO1, COBIT PO9, COBIT DS1, Val IT VG1	Key services and supporting business processes and systems
RE2.1	Risk analysis focus areas
RG1.5, RE3.2, RE3.4	Prioritised inventories of risk and impact categories

RG 1.4 Propose IT risk tolerance thresholds

From	Inputs
RG1.2	IT risk management methods
RG1.3	Key services and supporting business processes and systems
RG1.3, COBIT ME4	Enterprise appetite for IT risk
RG1.5	IT risk tolerance thresholds
*	Enterprise risk management framework
*	Business risk tolerance thresholds

To	Outputs
RG1.5	Proposed IT risk tolerance thresholds

RG 1.5 Approve IT risk tolerance

From	Inputs
RG1.3	Key services and supporting business processes and systems, prioritised inventories of risk and impact categories
RG1.3, COBIT ME4	Enterprise appetite for IT risk
RG1.4	Proposed IT risk tolerance thresholds

To	Outputs
RG1.4, RG1.6, RG1.7, RG3.3, RG3.4, RE2.2, RE2.3, RE3.2, RE3.5, RE3.6, RR2.2, RR3.2, COBIT PO9, *	IT risk tolerance thresholds

RG 1.6 Align policy and standards statements with IT risk tolerance

From	Inputs
RG1.2	IT risk management methods
RG1.5	IT risk tolerance thresholds
COBIT PO4	Technology standards
COBIT PO6	IT policies

To	Outputs
RG1.7, RG2.2, RG3.3, COBIT PO4, PO6, PO7, PO8, PO9	Updated policies and standards

RG 1.7 Promote an IT risk-aware culture

From	Inputs
RG1.1	IT risk management framework
RG1.5	IT risk tolerance thresholds
RG1.6	Updated policies and standards
RG1.8	Plans for ongoing IT risk communication
RG2.1	IT risk RACI charts
Val IT VG1	Leadership commitment
COBIT ME2	Report on effectiveness of IT controls
*	Risk culture survey results, data on adherence to policy and standards, data on IT risk thresholds vs. policy vs. operations

To	Outputs
RE1.5	Performance metrics on cultural shift toward risk awareness
COBIT PO6	IT-related risk management guidelines
COBIT DS7	Specific training requirements
*	Communication of risk principles and concepts

RG 1.8 Promote effective communication of IT risk

From	Inputs
RG3.3	Potential risk issues and opportunities
RR1.2	State of compliance reports
COBIT PO4	IT organisation and relationships

To	Outputs
RG1.7, RG3.4, RR3.2, COBIT PO6	Plans for ongoing IT risk communication
RG1.3	Request for enterprise-wide IT risk assessment

RG 1 RACI Chart

Key Activities	Board	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
RG1.1 Develop an enterprise-specific IT risk management framework.	A	R	R	R	C	I	R	I	C	I	C
RG1.2 Develop IT risk management methods.	C	C	A	R	C	I	C	C	C	I	C
RG1.3 Perform an enterprise-wide IT risk assessment.	I	A	R	R	C	I	R	C	R	C	C
RG1.4 Propose IT risk tolerance thresholds.	I	I	C	R	C	I	A	C	C		C
RG1.5 Approve IT risk tolerance.	A	C	C	C	C	R	C	C	C	C	C
RG1.6 Align policy and standards statements with IT risk tolerance.		I	A	R	I	C	R	I	C	R	I
RG1.7 Promote an IT risk-aware culture.	A	R	R	R	R	R	R	R	R	R	R
RG1.8 Promote effective communication of IT risk.	A	R	R	I	I	R	I	I	I	I	C

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

RG 1 Goals & Metrics

Activity Goals	Process Goal	RG Goal
• Establish enterprise-wide accountability for managing IT risk. • Establish accountability for IT risk issues. • Co-ordinate IT risk strategy and business risk strategy. • Adapt IT risk management practices to organisational risk management practices. • Provide adequate resources for IT risk management.	• Integrate the IT risk strategy and operations with the business strategic risk decisions that have been made at the enterprise level.	• Ensure that IT risk management practices are embedded in the enterprise, enabling the enterprise to secure optimal risk-adjusted return.

Activity Metrics	Process Metrics	RG Metrics
• Percentage of employees whose performance metrics and rewards reflect risk management objectives • An alignment score related to RACI regarding the ranking of actions to take (e.g., percentage of key IT risk-related accountabilities accepted by business and IT personnel) • Number of different risk reports provided to the board; extent of integration of reporting on IT risk • Percentage of IT risk practices adapted to ERM organisational expectations • Percent of IT risk management action plans approved for implementation • Percentage of core ERM activities with embedded IT risk considerations • Number of different issue management processes and platforms • Extent to which budgets are allocated based on risk significance (e.g., per risk assessment results) • Number of open positions in the risk management staff	• Percentage of business executives and managers who have received training on the enterprise's reliance on and usage of IT, the related risk, IT risk strategy and framework • Percentage of IT risk management operational expenditures that have direct traceability to business risk strategy • Percentage of business projects that consider IT risk • Percentage of core ERM activities that consider IT risk • Frequency of IT risk as an agenda item for the executive committee • Extent of alignment between organisational objectives and IT risk management objectives • Extent of overlap of risk management activities performed by business units, risk and control functions, and internal audit	• The degree to which the strategic use of IT in leveraging enterprise resources reduces overall enterprise risk • Percentage of staff trained in critical risk management techniques (e.g., standard risk analysis techniques, crisis management, project management, skills of people [audit, etc.] to detect when something IT related is amiss)

RG2: ERM Integration

- Process Goal:
  - Integrate the IT risk strategy and operations with the business strategic risk decisions that have been made at the enterprise level.
- Key Activities:
  - RG2.1 Establish enterprisewide accountability for managing IT risk
  - RG2.2 Establish accountability for IT risk issues
  - RG2.3 Coordinate IT risk strategy and business risk strategy
  - RG2.4 Adapt IT risk management practices to organisational risk management practices
  - RG2.5 Provide adequate resources for IT risk management

RG3: Risk Business Decisions

- Process Goal:
  - Ensure that organisational decisions consider the full range of opportunities and consequences from reliance on IT for success.
- Key Activities:
  - RG3.1 Gain management buy in for the IT risk analysis approach
  - RG3.2 Approve IT risk analysis results
  - RG3.3 Embed IT risk considerations into strategic business decision making
  - RG3.4 Accept IT risk
  - RG3.5 Prioritise IT risk response activities
  - RG3.6 Track key IT risk decisions

RG Defined - 3

- IT risk management is viewed as a business issue, and both the downside and upside of IT risk are recognised. There is a designated leader for IT risk across the enterprise; this leader is engaged with the enterprise risk committee, where IT risk is in scope and discussed. The business understands howIT fits in the enterprise-wide, or portfolio view, risk perspective. Enterprise risk tolerance is derived from local tolerances and IT risk management activities are being aligned across the enterprise. Formal risk categories have been identified and described in clear terms. Risk awareness training includes situations and scenarios beyond specific policy and the structures and a common language for communicating risk. Defined requirements exist for a centralised inventory of risk issues. Workflow tools are used to escalate risk issues and track decisions.

Risk Evaluation

- Domain Goal:
  - Ensure that IT related risks and opportunities are identified, analysed, and presented in business terms.
- Domain Metric:
  - The cumulative business impact from IT-related incidents and events not identified by risk evaluation processes.

RE1: Collect Data

- Process Goal:
  - Identify relevant data to enable effective IT related risk identification, analysis, and reporting.
- Key Activities:
  - RE1.1 Establish & maintain a model for data collection
  - RE1.2 Collect data on the external environment
  - RE1.3 Collect timely event, incident, problem and loss data
  - RE1.4 Identify risk factors
  - RE1.5 Organize historical IT risk data

RE2: Analyze Risk

- Process Goal:
  - Develop useful information to support risk decisions that take into account the business relevance of risk factors (e.g., threats, vulnerabilities, value, liability).
- Key Activities:
  - RE2.1 Define IT risk analysis scope
  - RE2.2 Estimate IT risk to and from critical products, services, processes, and IT resources
  - RE2.3 Identify risk response options
  - RE2.4 Perform a peer review of IT risk analysis results

RE3: Maintain Risk Profile

- Process Goal:
  - Maintain an up-to-date and complete inventory of known risks and attributes (e.g., expected frequency, potential impact, disposition), IT resources, capabilities and controls as understood in the context of business products, services, and processes.
- Key Activities:
  - RE3.1 Map IT resources to business processes
  - RE3.2 Determine the business criticality of IT resources
  - RE3.3 Understand IT capabilities
  - RE3.4 Connect threat types & business impact categories
  - RE3.5 Maintain the IT risk register and IT risk map
  - RE3.6 Design and communicate IT risk indicators

RE Defined – 3

- There is an emerging understanding of risk fundamentals. Gaps between IT-related risk and opportunity and overall risk appetite are being recognised. Responsibility and accountability for key risk evaluation practices are defined and process owners have been identified. The capability is in place to evaluate IT risk on an enterprise-wide basis alongside other risk types. Dependency analysis and scenario analysis procedures are defined and performed across multiple business activities, business lines and products. Skill requirements are defined and documented for all enterprise risk areas, with full consideration of data collection, risk analysis and profiling. Data collection tools generally adhere to defined standards and distinguish between threat events, vulnerability events and loss events.

Risk Response

- Domain Goal:
  - Ensure that IT-related risk issues, opportunities, and events are addressed in a cost effective manner and in line with business priorities.
- Domain Metrics:
  - The cumulative business impact from IT-related incidents and events anticipated by risk evaluation processes but not yet addressed by mitigation or event action planning.

RR1 Articulate Risk

- Process Goal:
  - Ensure that information on the true state of IT-related exposures and opportunities is made available in a timely manner and to the right people for appropriate response.
- Key Activities:
  - RR1.1 Report IT risk analysis results
  - RR1.2 Report IT risk management activities and state of compliance
  - RR1.3 Interpret external IT assessment findings
  - RR1.4 Identify IT-related opportunities

RR2 Manage Risk

- Process Goal:
  - Ensure that measures for seizing strategic opportunities and reducing risk to an acceptable level are managed as a portfolio.
- Key Activities:
  - RR2.1 Inventory controls, capabilities, and resources
  - RR2.2 Monitor operational alignment with risk tolerance thresholds
  - RR2.3 Respond to discovered risk exposure and opportunity
  - RR2.4 Implement controls
  - RR2.5 Report on IT risk action plan progress

RR3 React to Events

- Process Goal:
  - Ensure that measures for seizing immediate opportunities or limiting the magnitude of loss from IT related events are activated in a timely manner and are effective.
- Key Activities:
  - RR3.1 Maintain incident response plans
  - RR3.2 Monitor IT risk
  - RR3.3 Initiate incident response plans
  - RR3.4 Conduct post mortem reviews of IT-related incidents

RR Defined – 3

- Across the enterprise there is individual understanding of business-impacting threats and the specific actions to take if the business threat materialises. Responsibility and accountability for key risk response practices are defined and process owners have been identified. Control deficiencies are identified and remediated in a timely manner. An enterprise-wide risk response policy defines when and how to respond to risk. Job descriptions include expectations for risk response. Employees are periodically trained in IT-related threats, risk scenarios, and controls relevant to their roles and responsibilities. A plan has been defined for use and standardisation of tools to automate certain risk mitigation activities, such as user provisioning.

Also available …

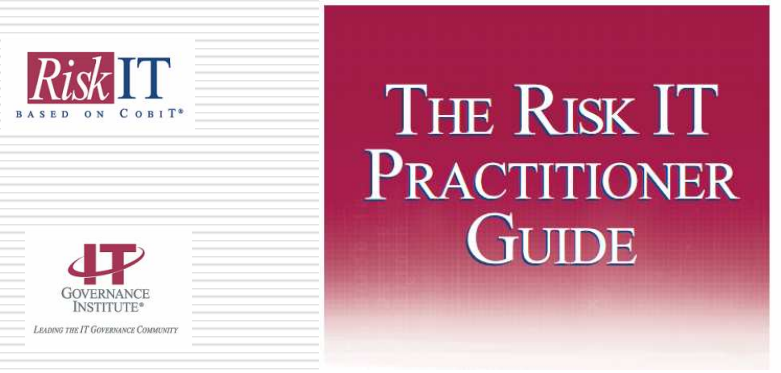
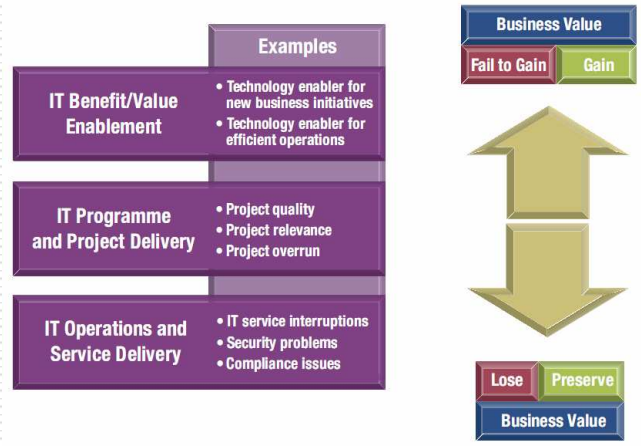


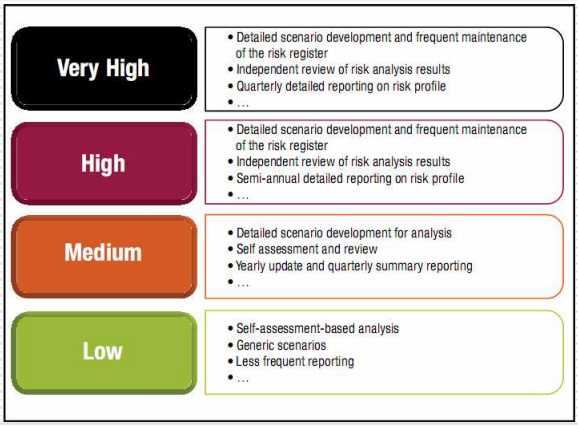
Table of Contents

- Defining a Risk Universe and Scoping Risk Management
- Risk Appetite and Risk Tolerance
- Risk Awareness, Communication and Reporting
- Expressing and Describing Risk
- Risk Scenarios
- Risk Response and Prioritization
- Risk Analysis Workflow
- Mitigation of IT Risk Using CobiT and Val IT

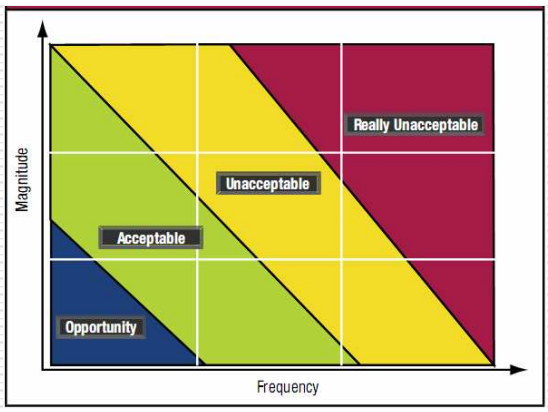
Types of IT Risk



IT Risk Management Scope

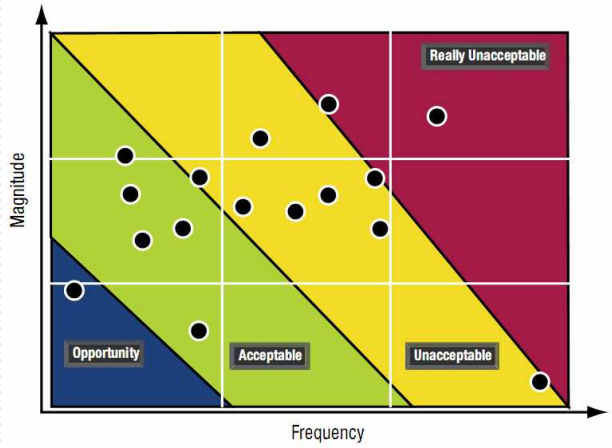


Risk Appetite Bands

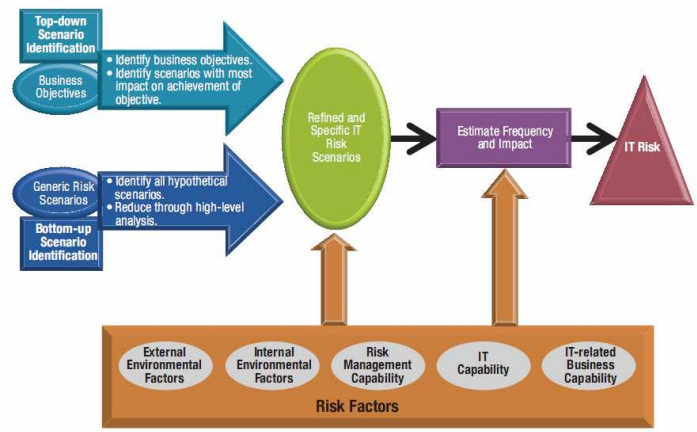


Risk Awareness, Communication and Reporting

Risk and Risk Appetite Map

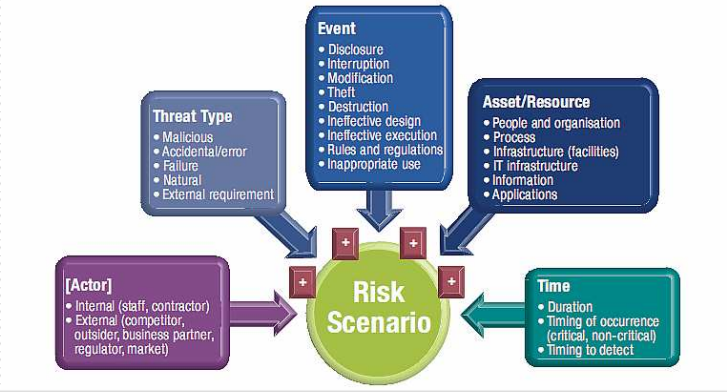


Risk Scenario Development



Risk Factors

Risk Scenario



30 Scenario Examples PT I

1. IT Project Selection
2. New technologies
3. Technology Selection
4. IT Investment Decision Making
5. Accountability over IT
6. Integration of IT within business processes
7. State of infrastructure technology
8. Ageing of application software
9. Architectural agility and flexibility
10. Regulatory compliance
11. Software implementation
12. IT Project Termination
13. IT Project Economics
14. Project Delivery
15. Project Quality

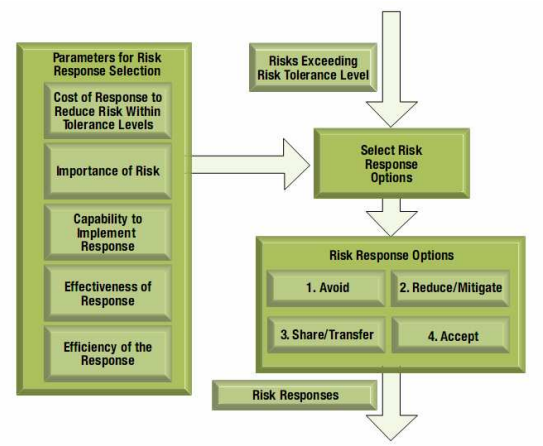
30 Scenario Examples PT II

16. Selection /Performance of third party suppliers
17. Infrastructure theft
18. Destruction of infrastructure
19. IT staff
20. IT expertise & skills
21. Software integrity
22. Infrastructure (Hardware)
23. Software performance
24. System Capacity
25. Ageing of infrastructural software
26. Malware
27. Logical attacks
28. Information Media
29. Utilities performance
30. Industrial action

New Technology Risk Scenario

- Failure to adopt and exploit new technologies (i.e., functionality, optimization) on a timely basis [minus]
- New and important technology trends not identified [minus]
- Inability to use the technology to realize desired outcomes (e.g., failure to make required business model or organizational changes) [minus]
- New technologies for new initiatives or more efficient operations adopted and exploited [plus]

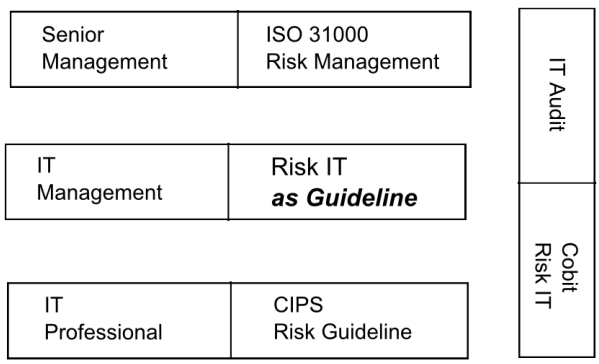
Risk Response Options



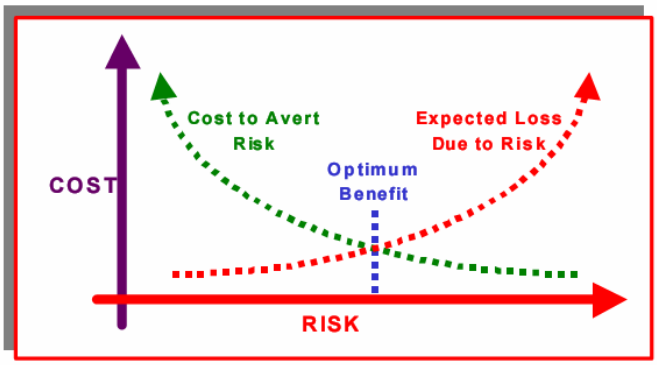
Other Standards/Frameworks

Principle/Feature	Risk IT		COSO ERM–Integrated Framework, 2004	ISO/FDIS 31000:2009	AS/NZS 4360:2004	ARMS, 2002		ISO 20000: 2005, Parts 1 and 2	PMBOK	ISO/IEC 27006:2008 ISO/IEC 27001:2005 ISO/IEC 27002:2005
Risk IT Principles										
Always connect to business objectives	■		■	■	■	■		▒	■	■
Align the management of IT-related business risk with overall ERM	■		▒	▒	▒	▒				▒
Balance the costs and benefits of managing risk	■		■	■	■	■				▒
Promote fair and open communication of IT risk	■		■	■	■	■				▒
Establish the right tone from the top while defining and enforcing personal accountability for operating within acceptable and well-defined tolerance levels	■		■	■	■	■			▒	■
Are a continuous process and part of daily activity	■		■	■	■	■		■	■	■
Additional Features										
Availability (to the general public)	■		▒	▒	▒	■		▒	▒	▒
Comprehensive view on IT (related) risk	■									▒
Dedicated focus on risk management practices for specific IT areas (project management, service management, security, etc.)	▒							■	■	■
Provide a detailed process model with management guidelines and maturity models	■		▒	▒	▒	▒		▒	▒	▒

Revised IT Audit World



Remember: Focus on Net Benefit



From: US Air Force - GSAM version 3.0

Thank You

… questions, comments?