The ITGI Framework

Toronto – 2009.10.15 – Bob Fabian

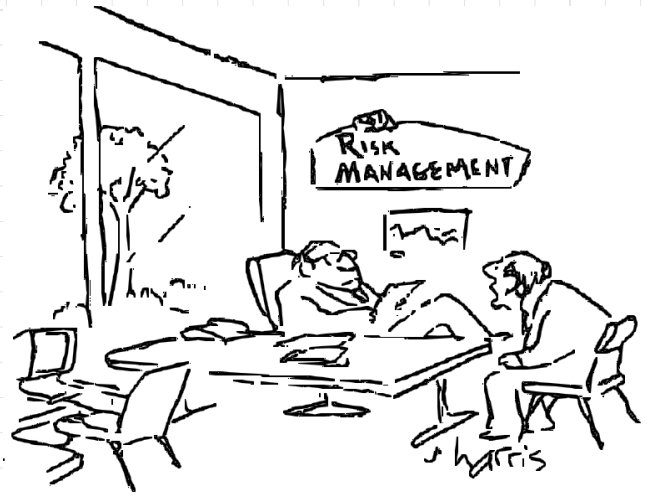
Plan

- Introduction
- Risk Context
- ITGI Context
- Risk IT
  - ITGI Risk Plans
  - Risk IT Structure
  - Domains
  - Process Example
  - Techniques
- Tomorrow

General Approach

- Covering all the details unwise
  - No way to cover it *all*
  - Framework - must customize
- Approach
  - Provide context
  - Explain framework
  - Sample details

We've advanced, … some



"Be Careful." All you can say is "Be Careful"?

Me, then You, ... then Risk

- 30+ years – IT methodologies
- Best Practice sea change
- Recent steps
  - Led: CIPS Risk Management Guideline
  - Organized: itSMF National Conferences
  - Member: Toronto COBIT User Group
  - "Expert Reviewer" – ITGI Risk IT

You ...

- Around the room -
  - Why are you here?
  - What's your IT background?
  - What's your risk background?
  - What do you want from this session?

Too Much Truth?

Denver's Old Airport

- Serious limit to growth

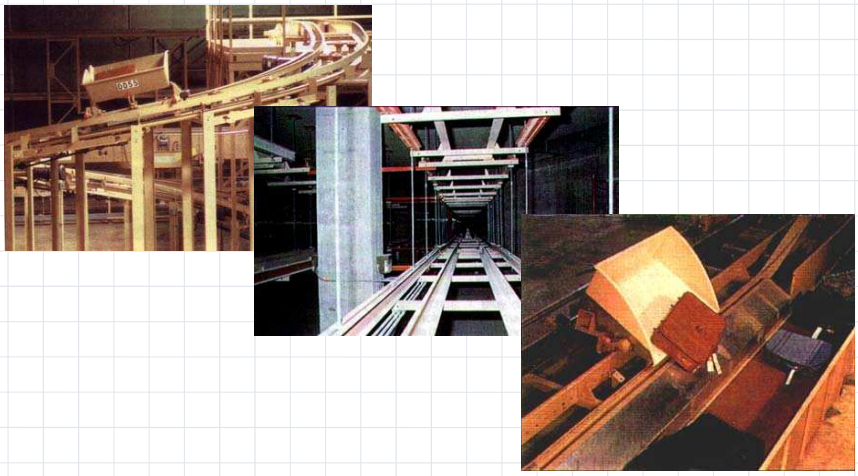
Denver's Grand Plan

- World's largest, most advanced design

Baggage Handling System

- Critical to fast turn-around for planes
- Old tug-and-cart system labor intensive
- New system to be "unique in complexity, technology and capacity"
- Untouched by human hands
  - 300 OS/2 computers
  - 14 million feet of wiring
  - 22 miles of track
  - 3,500 telecarts

Baggage Handling at Work



Time Line – Baggage Handling

- Nov ’89 – Airport construction begins
- Apr ’92 – Design/build contract signed
- Feb ’93 – Opening delayed to Mar ’94
- Apr ’94 – Disaster at first public test
- Feb ’95 – Airport finally opened
- Aug ’05 – Tug-and-cart wins out!

One Description

- The $234 million project cost roughly $1 million per day in lost operations and interest on bond issues. In tests, bags were misloaded, misrouted, or fell out of telecarts. The system continued to unload into jammed conveyor belts, and loaded telecarts that were full. Recovery failed to recognized loaded telecarts. Timing was not synchronized, causing bags to fall between the conveyor belt and telecarts. Agh!

http://www.cds.caltech.edu/conferences/1997/vecs/tutorial/Examples/Cases/failures.htm

Risk Management, NOT!

- Overall airport project
  - Begin construction with no fixed BHS
  - Select advanced state-of-the-art system
  - Failure to provide fallback alternative
- Baggage handling system
  - Failure to run full system simulation
  - Failure to enforce all contract provisions
  - Weak failsoft and recovery procedures

Grand Design, but …

What would you have done?

- Critically important contract for a small specialized firm
- Very strict contract provisions giving project priority over everything else
- BUT
  - Chief project support dies within a month
  - Multiple clients, frequent scope changes
  - No ability to enforce contract provisions

References

- *BAE Automated System (parts A & B): Denver International Airport Baggage-Handling System*, HBR Case Study 9-396-311,312, Montealegre, Nelson, Knoop, and Applegate, Nov 1996
- *The Baggage System at Denver: Prospects and Lessons*, Richard de Neufville, Journal of Air Transport Management, Dec 1994
- *The Denver International Airport Automated Baggage Handling System*, MIS 611 Group Project, Bainum, Ji, and Kheny, Winter 2005,
- *Denver International Airport Reconsidered*, Chapter 3, *Waltzing with Bears*, DeMarco and Lister, Dorset House, 2003
- *Denver Airport Saw the Future. It Didn't Work*, Kirk Johnson, NYTimes, Aug 27, 2005
- *United axes troubled baggage system at Denver airport*, Todd Weiss, ComputerWord, June 10, 2005

  - Photos: airchive.com, howstuffworks.com, denver.org

Risk Free Project

A risk free project isn't worth doing!

- Only one explanation:
  - It's not going to deliver any value, otherwise it would already have been done

for Project Risk Management

- Makes aggressive risk-taking possible
- Decriminalizes risk
- Sets up projects for success
- Bounds uncertainty
- Provides minimum-cost downside protection
- Protects against invisible transfer of responsibility

for Project Risk Management – II

- Can save part of a failed effort
- Maximizes opportunity for personal growth
- Protects management from getting blindsided
- Focuses attention where it is needed

Waltzing with Bears, DeMarco & Lister

against Project Risk Management

- We're not mature enough to face up to risk
- Extent of uncertainty is just too much
- Uncertainty excuses poor performance
- "Manage for Success" is better
- We don't have the data to manage risks
- It's dangerous to be the first risk manager

Waltzing with Bears

Bottom of Totem Pole

- We're all professionals
  - Aren't we?
- Professionals have an obligation to provide trustworthy competence
- Paying attention to risk best practices a key part of that obligation

Best Practice Sea Change

- Previously (10+ years ago)
  - Best Practice "Standards"
    - Focused on HOW, some what, little why
  - Not very practical
- Today
  - Best Practice Guidelines
  - Focus on WHAT, some why, less how
  - Can be very practical

Professional Basic

- Who can a client (the public) trust?
- Professionals => Trustworthy
  - Trustworthy intentions
    - Committing to professional ethics
    - Understanding what client values
  - Trustworthy competence
    - Knowledge of technology
    - Knowledge of process
- Should be a win-win-win!
    - Client, professional, profession

Professional

- Requirement to be *trustworthy*
  - Trustworthy Intentions
  - Trustworthy Competence
- Best Practices key to Trustworthy Competence
  - Must always be considered

Trustworthy Process

- Deliver max value/min risk
- Except:
  - Value determined by client
  - Risk impact determined by client
  - Risk appetite/tolerance varies
- Optimize value/risk balance

Risk Management

- *The* professional responsibility
  - Clients can recognize value
  - But may not appreciate risk
- Professional responsibility
  - Before: Assess Risks
  - During: Manage Risks
  - Always: Communicate

Risk Management Hierarchy

Next Step

- Individual risk management
- Target: IT Risk Management
- Context: Corporate Risk Management
- OCEG: "Red Book"
  - Important GRC framework
    - Governance
    - Risk Management
    - Compliance

Recent Financial "Problems"

- Motivation
  - Massive financial rewards for successfully taking risks with other people's money; minimal penalties for failure.
- Technical
  - Assumption that "packaged" risks will be less risky than the individual risks. Self-delusional.

Public Perception

- Risk is longer under the TLC of the quants (math/finance types)
- Risk, and risk taking, are very public
- Heads have rolled
- More heads will roll
- Boards are paying attention
  - [They don't really have an option!]

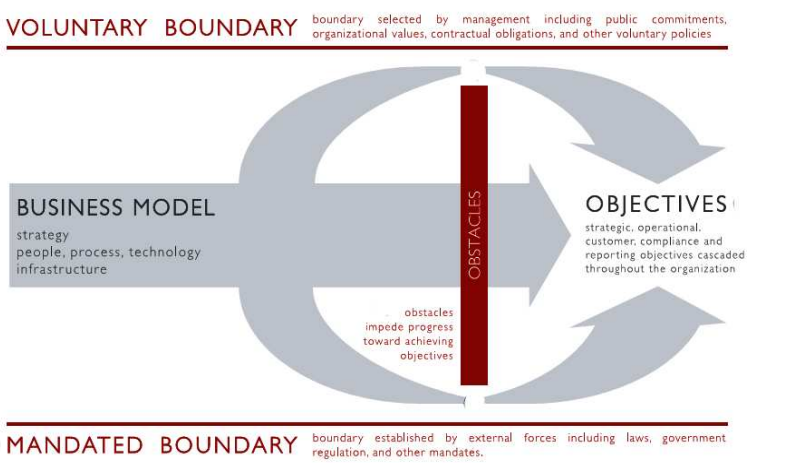
What the Board reads

- COSO on Risk
  - Committee of Sponsoring Organizations – *the* Sarbanes-Oxley reference material
- Open Compliance & Ethics Group
  - Very high profile group concerned with governance, risk, and compliance
  - (We'll use OCEG to explore corporate risk context)

COSO View

- "Every entity exists to provide value for its stakeholders. All entities face uncertainty, and the challenge for management is to determine how much uncertainty to accept as it strives to grow stakeholder value."

OCEG v1 Model



OCEG "Red Book"

OCEG Charter Leadership

CISCO · Deloitte. · Ernst & Young Quality In Everything We Do · Littler · LRN
SAP · Global Compliance · AON · DELL · ethics·point · MARSH
Microsoft · ORACLE · Grant Thornton A passion for the business of accounting · Qwest Spirit of Service · MetricStream
PricewaterhouseCoopers

OCEG's GRC - 1

- Governance
  - Culture, values, mission, structure and layers of policies, procedures and measures by which organizations are directed and controlled. Governance includes but is not limited to the activities of the Board, for governance bodies at various levels throughout the organization also play a critical role.

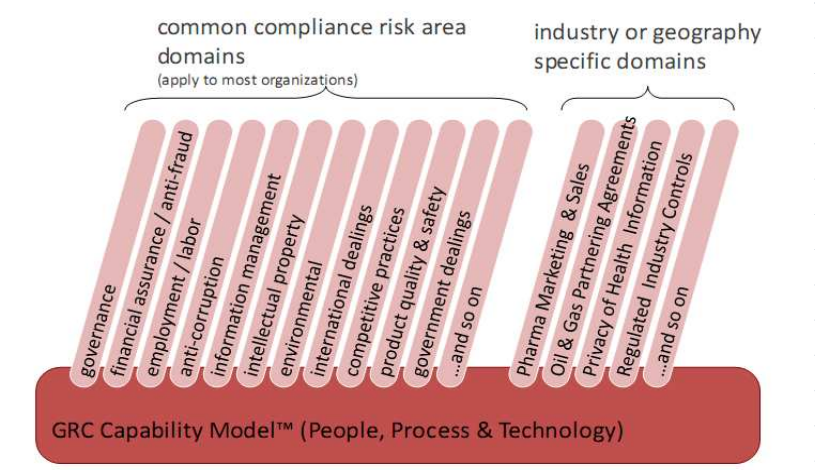
OCEG's GRC - 2

- Risk
  - The measure of the likelihood of something happening that will have an effect on achieving objectives; most importantly, but not exclusively, an adverse effect. Risk Management is the systematic applications of processes and structure ... to realize potential opportunities while managing adverse effects of risk.

OCEG's GRC - 3

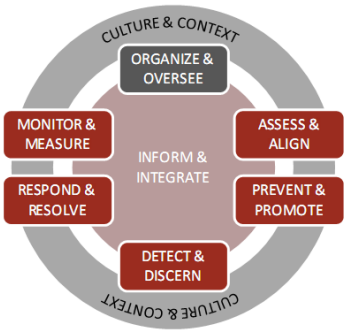
- Compliance
  - The act of adhering to, and the ability to demonstrate adherence to, mandated requirements defined by laws and regulations, as well as voluntary requirements resulting from contractual obligations and internal policies.

OCEG Capability Model



OGEC Big Picture

8 INTEGRATED COMPONENTS



8 UNIVERSAL OUTCOMES

- Achieve Business Objectives
- Enhance Organizational Culture
- Increase Stakeholder Confidence
- Prepare & Protect the Organization
- Prevent, Detect & Reduce Adversity
- Motivate & Inspire Desired Conduct
- Improve Responsiveness & Efficiency
- Optimize Economic & Social Value

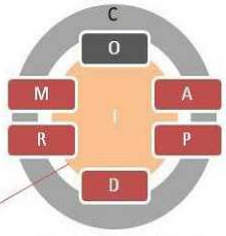
OGEC Component Model

MONITOR & MEASURE
M1 – Context Monitoring
M2 – Performance Monitoring & Evaluation
M3 – Systemic Improvement
M4 – Assurance

RESPOND & RESOLVE
R1 – Internal Review & Investigation
R2 – Third-Party Inquiries & Investigations
R3 – Corrective Controls
R4 – Crisis Response & Recovery
R5 – Remediation & Discipline

INFORM & INTEGRATE
I1 – Information Mgt & Documentation
I2 – Int.& Ext. Communication
I3 – Technology & Infrastructure

CONTEXT & CULTURE
C1 – External Business Context
C2 – Internal Business Context
C3 – Culture
C4 – Values & Objectives



DETECT & DISCERN
D1 – Hotline & Notification
D2 – Inquiry & Survey
D3 – Detective Controls

ORGANIZE & OVERSEE
O1 – Outcomes & Commitment
O2 – Roles & Responsibilities
O3 – Approach & Accountability

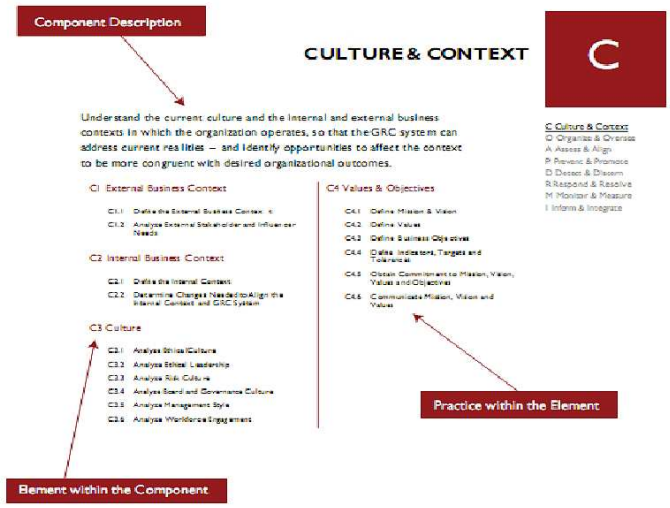
ASSESS & ALIGN
A1 – Risk Identification
A2 – Risk Analysis
A3 – Risk Optimization

PREVENT & PROMOTE
P1 – Codes of Conduct
P2 – Policies
P3 – Preventive Controls
P4 – Awareness & Education
P5 – Human Capital Incentives
P6 – Stakeholder Relations & Requirements
P7 – Risk Financing / Insurance

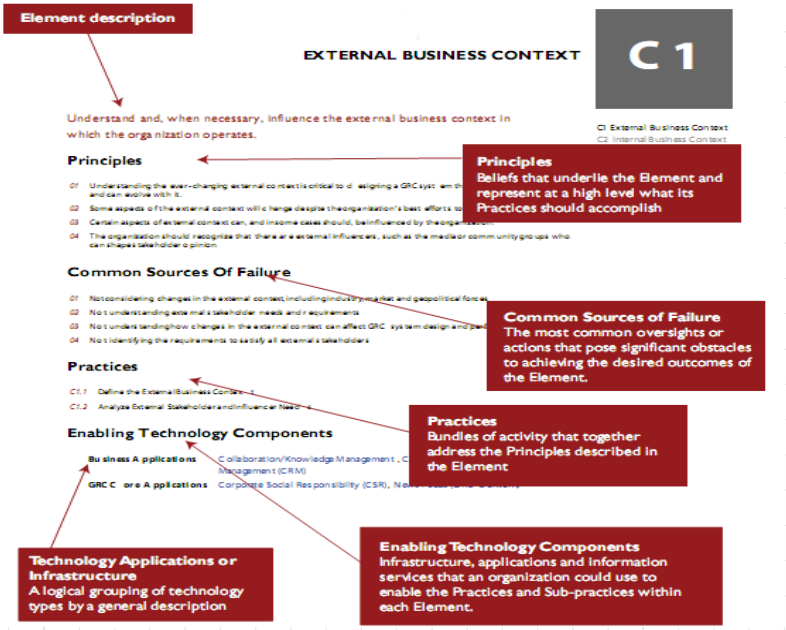
Model Elements

- Element Principles
- Common Sources of Element Failure
- Element Practices
  - Sub-Practices
- Related Requirements
- Key Deliverables
- Technology for (Sub-)Practices

Component Pages

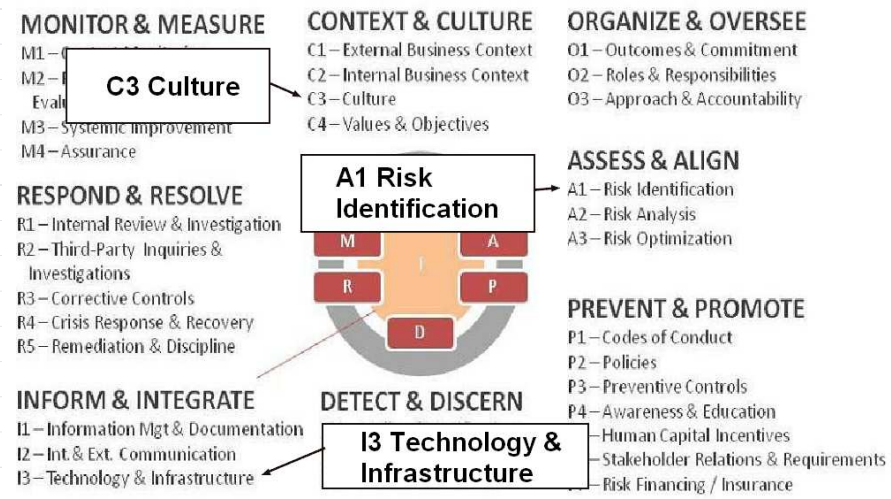


Element Pages



Practice Pages

Selected Elements



C3 Culture Principles

- Top leadership sets the tone
- Leadership must convince individuals they are sincere
- GRC will often need to change culture
- GRC must monitor culture for undesirable changes

C3 Culture Failure

- Not considering culture as it really exists prior to change
- Not realizing there are often many "sub cultures", each of which views risk, value, and communication differently

C3 Culture Practices

- Analize ethical culture
- Analize ethical leadership
- Analize risk culture
- Analize Board & Governance Culture
- Analize Management Style
- Analize Workplace Engagement

C3 Culture Key Deliverable

- GRC Strategic Plan

C3.1 Ethical Culture

- Periodically sample emplyees
  - Values/Principles perceptions
  - Procedures to raise issues
  - Pressure to be unethical
- Identify communication messages
  - Importance of values/principles
  - Importance of raising issues
  - Freedom from retaliatioin
- Define targets and measures

C3.2 Ethical Leadership

- Regularly sample workforce perceptions
  - Models ethical behaviour
  - Links ethics to performance
- Ethics importance in selecting leaders
- Are new leaders trained in ethics
- Define targets and measures
- Nurture appropriate succession plan

C3.3 Risk Culture

- Regularly sample workforce
  - Is risk appetitie communicates
  - Are leadership models appropriate
  - Are individuals able to handle risk
- Define desired risk state
- Define targets & measures

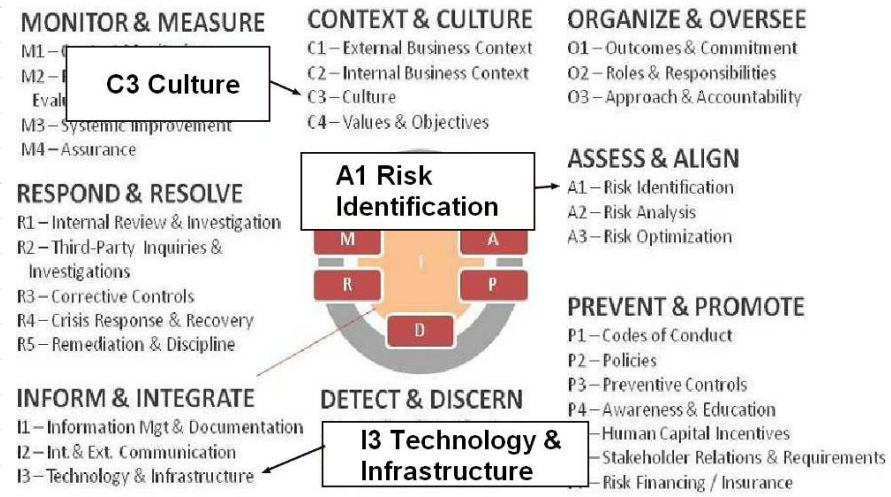
C3.4 Board & Governance

- Ask the Board
  - Can members raise issues
  - Can management be challenged
  - Is Board effective
- Ask Management
  - Is Board effective
  - Is Board engaged
- Judge active vs. passive

C3.5 Management Style

- How is decision-making authority delegated
- How are authority & accountability assigned & enforced
- How formal/informal is management
- Centralize/Decentralize philosophy

Selected Elements



A1 Risk Identification Principles

- Focus on key objectives, assets, and operations
- Bottom-up participation identifies what really happens
- Categorizing risks help to uniformly gather information
- Multi-faceted risks require multi-faceted responses

A1 Risk Identification Failure

- Not identifying all
  - Products or services
  - Geographies and locations
  - Legal and contractual requirements
- Not identifying risks faced by peers
- Not identifying new risks in timely way
- Not considering opportunities

A1 Risk Identification Practices

- Identify affected objectives & operations
- Identify changes that drive risk
- Identify integrity & culture risks
- Identify compliance, operational, & economic risks
- Identify risk opportunities
- Identify risk trends and connections

A1 Risk Identification Key Deliverable

- Prioritized Risk Matrix – document identified risks and their attributes:
  - Risk category
    - People, Things. Business Interruption, Civil or Criminal, Reputation, Quality, Economic
  - Related requirements
  - Nature of impacts
  - Roles affecting outcome

I3 Tech. & Infra. Principles

- Not everything can or should be automated
- Consistent tools are to be favored
- GRC plan benefits from IT involvement
- Should be partnership between GRC professionals and IT professionals

I3 Tech. & Infra. Failure

- Not knowing what technology is available to help with GRC
- Not understanding the available solutions
- Not using existing solutions/data to help with GRC
- Not including GRC technology in overall IT plan

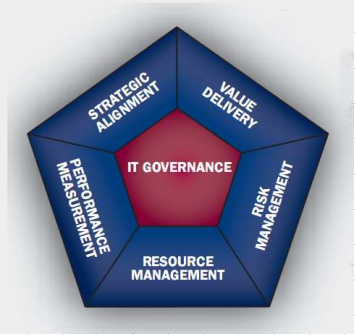
I3 Tech. & Infra.

- Practices
  - Assess technology needs and gaps
  - Develop GRC technology portion of GRC plan
- Key Deliverable
  - GRC strategic plan

Best Practices

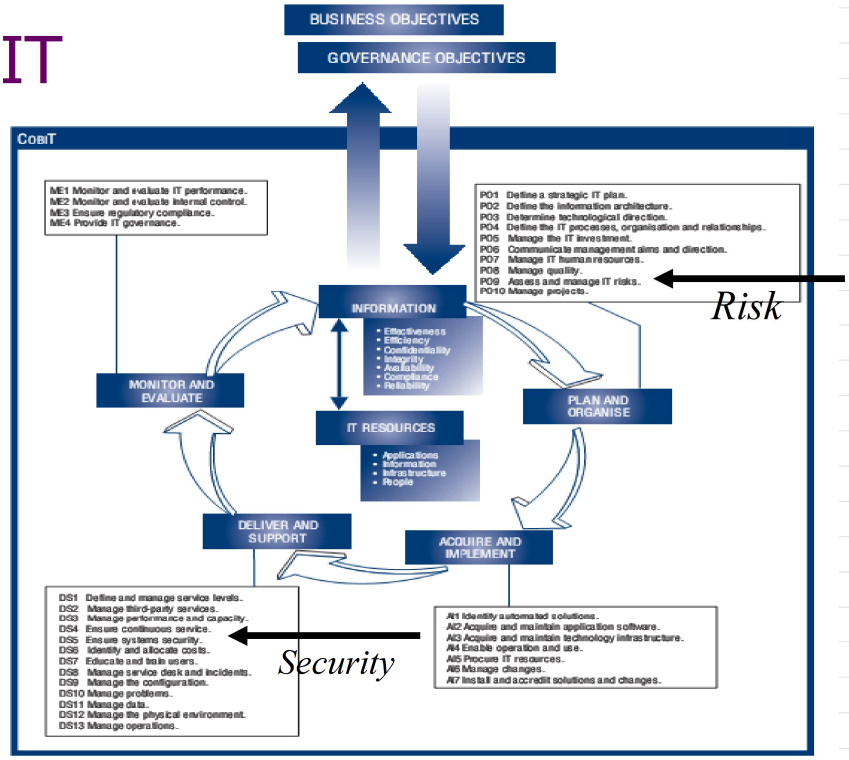
- They're now practical
- Professionalism requires their use
- COBIT is *the* IT best practice
- Risk is key COBIT process
- Risk IT is *the* detailed view of IT risk
- IT professionals need to understand Risk IT!

COBIT View

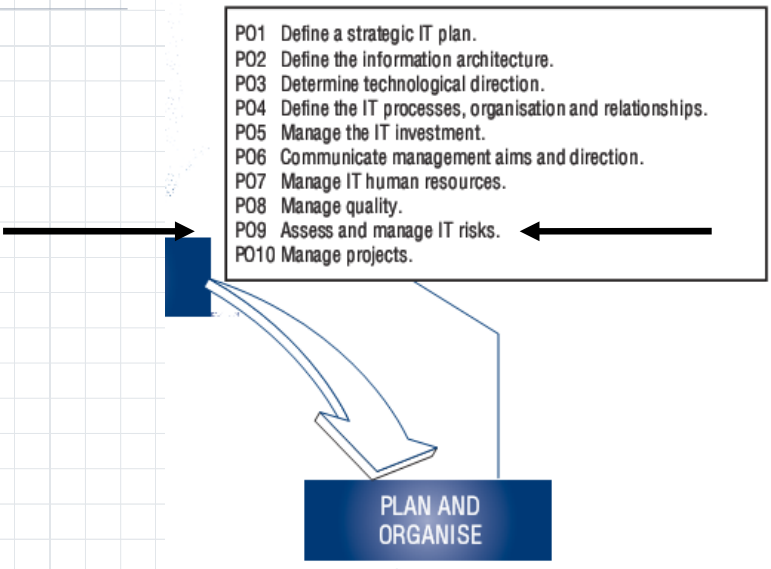


- Strategic alignment
- **Value delivery**
- Resource management
- **Risk management**
- Performance management

COBIT



Plan & Organize



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

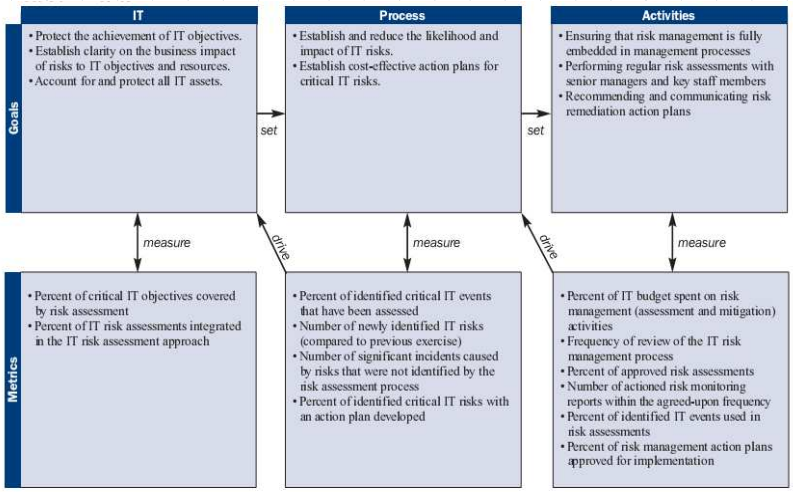
COBIT: Risk Input & Output

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 Mangement	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

1: Initial/Ad Hoc

"IT risks are considered in an *ad hoc* manner. Informal assessments of project risk take place as determined by each project. Risk assessments are sometimes identified in a project plan but are rarely assigned to specific managers. Specific IT-related risks such as security, availability and integrity are occasionally considered on a project-by project basis. IT-related risks affecting day-to-day operations are seldom discussed at management meetings. Where risks have been considered, mitigation is inconsistent. There is an emerging understanding that IT risks are important and need to be considered."

2: Repeatable but Intuitive

"An immature and developing risk assessment approach exists and is implemented at the discretion of the project managers. The risk management is usually at a high level and is typically applied only to major projects or in response to problems. Risk mitigation processes are starting to be implemented where risks are identified."

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."

4: Managed & Measured

"The assessment and management of risk are standard procedures. Exceptions to the risk management process are reported to IT management. IT risk management is a senior management-level responsibility. Risk is assessed and mitigated at the individual project level and also regularly with regard to the overall IT operation. Management is advised on changes in the business and IT environment that could significantly affect the IT-related risk scenarios. Management is able to monitor the risk position and make informed decisions regarding the exposure it is willing to accept. All identified risks have a nominated owner, and …"

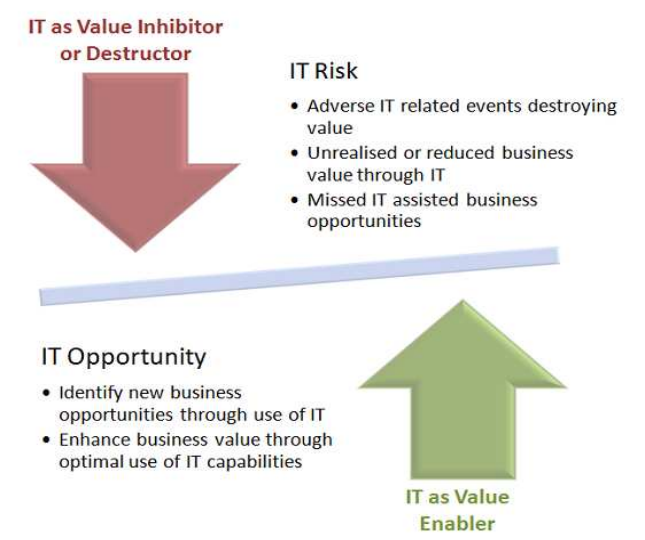
5: Optimised

"Risk management has developed to the stage where a structured, organisationwide process is enforced and well managed. Good practices are applied across the entire organisation. The capturing, analysis and reporting of risk management data are highly automated. Guidance is drawn from leaders in the field and the IT organisation takes part in peer groups to exchange experiences. Risk management is truly integrated into all business and IT operations, is well accepted, and extensively involves the users of IT services. Management will detect and act when major …"

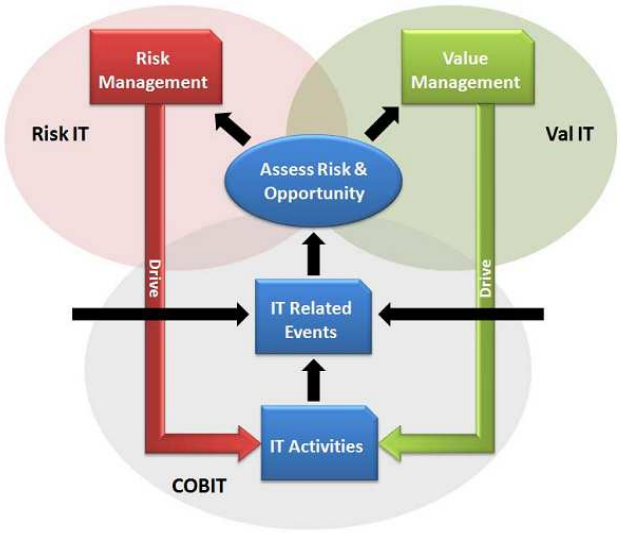
Time Line

- 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 about to be released
  - Timely
  - Completes the picture

Risk / Value Balance



Big 3 ITGI Frameworks



Real Soon Now …

Risk IT
BASED ON COBIT®

IT GOVERNANCE INSTITUTE®
LEADING THE IT GOVERNANCE COMMUNITY

ENTERPRISE RISK: IDENTIFY, GOVERN AND MANAGE IT RISK

The Risk IT Framework

EXPOSURE DRAFT

Risk IT Definition

- **IT risk** is business risk—specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise. It consists of IT-related events that could potentially impact the business. It includes both uncertain frequency and magnitude, and it creates challenges in meeting strategic goals and objectives as well as uncertainty in the pursuit of opportunities. IT risk can be categorised in different ways:
  - **IT service delivery risk**, associated with the performance and availability of IT services, and which can bring destruction or reduction of value to the enterprise
  - **IT solution delivery/benefit realisation risk**, associated with the contribution of IT to new or improved business solutions, usually in the form of projects and programmes
  - **IT benefit realisation risk**, associated with (missed) opportunities to use technology to improve efficiency or effectiveness of business processes, or to use technology as an enabler for new business initiatives
- IT risk always exists, whether or not it is detected or recognised by an organisation.

Risk IT Purpose

- "Management of business risk is an essential component of the responsible administration of any enterprise. Almost every business decision requires the executive or manager to balance risk and reward.
- "The pervasive use of IT can provide significant benefits to an enterprise, but it also involves risk. Due to IT's importance to the overall business, IT risk should be treated like other key business risks, such as market risk, credit risk and other operational risks, all of which fall under the highest 'umbrella' risk category: failure to achieve strategic objectives. While these other risks have long been incorporated into corporate decision-making processes, too many executives tend to relegate IT risk to technical specialists outside the boardroom."

Risk IT Audience & Benefit

Role	Benefits of/Reasons for Using the Risk IT Framework
Boards and executive management	Better understanding of their responsibilities and roles with regard to IT risk management
Corporate risk managers (for enterprise risk management)	Assistance with managing IT risk, in line with generally accepted enterprise risk management principles
Operational risk managers	Linkage of their framework to Risk IT; identification of operational losses or development of key risk indicators
IT management	Better understanding of how to identify and manage IT risk and how to communicate IT risk to business decision makers
IT service managers	Enhancement of their already good view of more operational IT-related risks, which should fit into an overall IT risk management framework
Business continuity managers	Alignment with enterprise risk management (since assessment of risk is a key aspect of their responsibility)
IT security managers	Positioning of security risk amongst other categories of IT risk
Chief financial officers (CFOs)	Gaining a better view of IT-related risk and its financial implications
Enterprise governance officers	Assistance with their review and monitoring of governance responsibilities and other IT governance roles
Business managers	Understanding and management of IT risk—one of many business risks, all of which should be aligned
IT auditors	Better analysis of risk in support of audit plans and reports
Regulators	Support of their assessment of regulated enterprises' IT risk management approach
External auditors	Additional guidance on IT-related risk levels when establishing an opinion over the quality of internal control
Insurers	Support in establishing adequate IT insurance coverage and seeking agreement on risk levels
Rating agencies	In collaboration with insurers; a reference to objectively assess and rate how an enterprise is dealing with IT risk

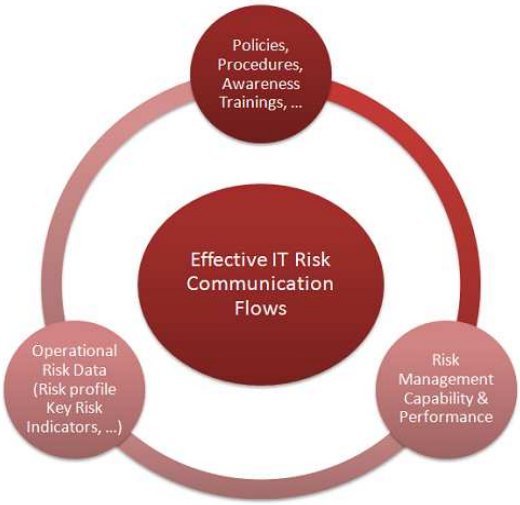
Risk IT Principles

- 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 of IT risk

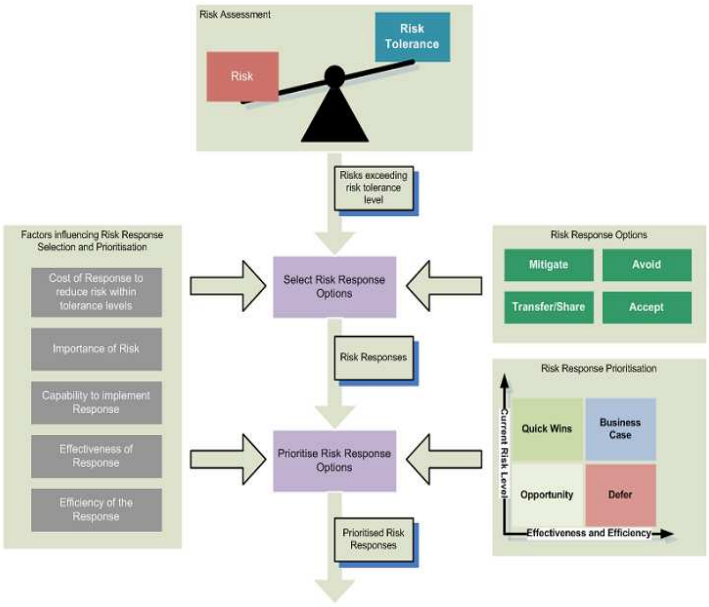
Risk IT Principles II

- Effective management 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
- 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 Communication

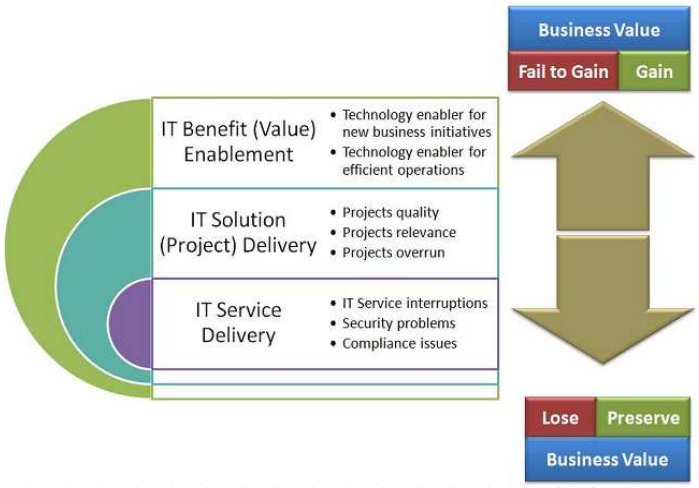


Response Approach

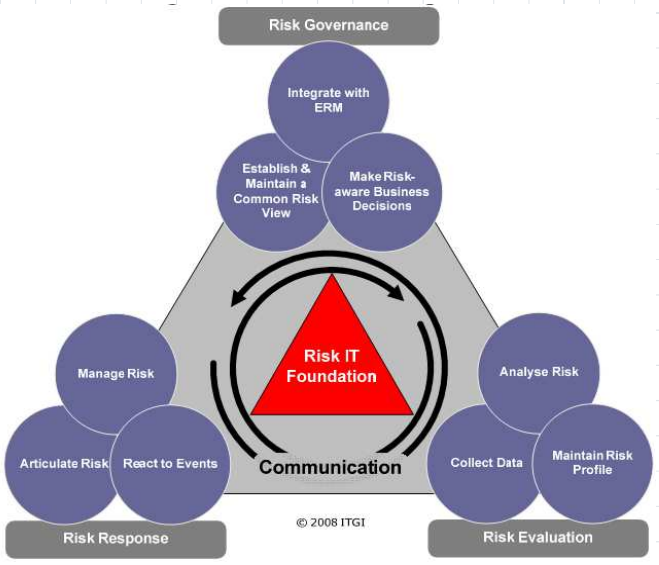


Risk Scenario

Types of IT Risk



Risk IT Overview



Three 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 Initial - 1

- There is an emerging understanding that IT risk is important and needs to be managed, but it is viewed as a technical issue and the business primarily considers the downside of IT risk. Any IT risk identification criteria vary widely across the enterprise and the IT organisation. By default, IT is accountable for problem management, availability, system access, etc. Risk appetite and tolerance are considered only during episodic risk assessments. Enterprise policies and standards, which are minimal at best, may be incomplete and/or reflect only external requirements and lack defensible rationale and enforcement mechanisms. IT risk management skills may exist on an ad hoc basis, but they are not actively developed. Ad hoc control-centric inventories are dispersed across desktop applications.

RG Repeatable - 2

- There is an awareness of the need to actively manage IT risk, but the focus is on technical compliance with no anticipation of value added. There are emerging leaders for IT risk management within silos who assume responsibility and are usually held accountable, even if this is not formally agreed. Risk tolerance is set locally and may be difficult to aggregate. Investments are focused on specific risk issues within functional and business silos (e.g., security, business continuity, operations). There is board-issued guidance for risk management. Minimum skill requirements, which include an awareness of IT risk, are identified for critical enterprise risk areas. Functional and IT silo-specific inventories of risk issues exist.

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.

RG Managed - 4

- IT risk management is viewed as a business enabler, and both the downside and upside of IT risk are understood. The designated leader for IT risk across the enterprise is fully engaged with the enterprise risk committee, which expects value from including IT in decisions. The IT department's role in operational risk management and the broader enterprise risk management is well understood. The board defines risk appetite and tolerance for all departments, including IT risk. Enterprise policies and standards reflect business risk tolerance. Far-sighted risk scenarios consider IT risk across the enterprise. Major risk decisions fully consider the probability of loss and the probability of reward. Skill requirements are routinely updated for all areas, proficiency is ensured for all risk management areas and certification is encouraged. Tools enable enterprise risk portfolio management, automation of IT risk management workflows, and monitoring of critical activities and controls.

RG Optimized - 5

- Senior executives make a point of considering all aspects of IT risk in their decisions. The IT risk leader is considered a trusted advisor during design, implementation and steady-state operations. The IT department is a major player in business line operational risk efforts and enterprise-wide risk efforts. Strategic objectives are based on an executive-level understanding of IT-related business threats, risk scenarios and competitive opportunities. Enterprise policies and standards continue to reflect business risk tolerance while increasing efficiency. The enterprise formally requires continuous improvement of IT risk management skills, based on clearly defined personal and organisational goals. Real-time monitoring of events and control exceptions exists, as does automation of policy management.

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 Initial – 1

- Recognition of the need for risk evaluation is emerging; however, there is minimal understanding of the business environment and the associated threats end events that may affect performance. By default, IT is accountable for risk evaluation. Current IT risk information and mitigation options are inferred from episodic assessments. Any data collection and analysis methods are ad hoc and may be compliance-driven. IT risk analysis skills may exist on an ad hoc basis, but they are not actively

RE Repeatable – 2

- Worst-case loss scenarios are the focus of discussions, although the driving factors for those scenarios may not be understood. Individuals assume responsibility for both risk evaluation and risk response. Some planned risk analysis occurs, but practitioners make major assumptions about the contributing factors for risk. Dependency analysis and scenario analysis are ad hoc and focus on only a limited number of business activities. Minimum skill requirements are identified for critical areas of data collection, risk analysis and risk profiling. Functional and IT silo-specific risk analysis approaches and tools exist but are based on solutions developed by key individuals.

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.

RE Managed – 4

- 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.

RE Optimized – 5

- Decision makers enjoy transparency into IT risk and have available the best possible information about loss probabilities, emerging exposures and opportunities. The drivers of the real risks to real operations are vigorously communicated throughout the extended enterprise. Employees at every level take direct responsibility for determining the business relevance of risk factors. The enterprise maintains an optimal balance between the qualitative and quantitative methods that support decisions on managing uncertainties and seizing risky opportunities. Risk evaluation activities are based on a broad and deep set of IT risk scenarios that integrate all business activities, business lines, products and known risk types. The enterprise formally requires continuous improvement of data collection, risk analysis and profiling skills. Automated tools enable end-to-end support and improvement of risk evaluation efforts.

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 Initial – 1

- Recognition of the need for risk response is emerging, but it is viewed as limited to risk avoidance, meeting compliance requirements and transfer through insurance. There is minimal individual awareness of threats and what to do when they materialise. There is minimal accountability for ensuring that reasonable risk response measures are in place and reflect the threat environment and asset values. IT-related events and conditions that could affect day-to-day operations are occasionally discussed at management meetings, but specific risk responses are not considered. IT controls exist but are based on compliance requirements, vary widely in relation to risk and operate in isolated silos. A lack of skills and competency for risk response may force the enterprise to accept risk beyond tolerance levels when value propositions are particularly compelling.

RR Repeatable – 2

- There is individual awareness of threats and points of contact for direction when they materialise. IT risk response issues are communicated by management but IT risk response discussions may be impaired by competing business unit-specific risk language. There is an emerging leader for IT risk response who assumes responsibility for mitigating risk and helping to manage the impact of events. Control deficiencies may be identified but are not remediated in timely manner. Risk mitigation processes are starting to be implemented where IT risk issues are identified. Minimum skill requirements are identified for critical areas of risk articulation, mitigation and crisis management. Common approaches to the use of risk mitigation and response tools exist but are based on solutions developed by key individuals.

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.

RR Managed - 4

- There is both individual and organisational understanding of the full requirements for responding to risk. Senior business management and IT management together determine whether a risk condition exceeds defined risk tolerances. A reward culture is in place that motivates positive action. The efficiency and effectiveness of risk response are measured and communicated, and linked to business goals and the IT strategic plan. All aspects of the risk response process are documented and quantitatively managed. Skill requirements are routinely updated for all risk response areas, including risk articulation, risk mitigation, reacting to events and seizing opportunities. Tools are being used in main areas to enable enterprise risk portfolio management and to monitor critical controls, capabilities and resources.

RR Optimized – 5

- The extended enterprise is well aware of the full requirements and the strategies and plans in place for responding to risk. The responses to real risks to real operations are vigorously communicated throughout the extended enterprise. The enterprise as whole collaborates with external entities to respond to common and pandemic risk issues. The enterprise measures the effectiveness of risk response efforts both internally and in collaboration with external entities. The full range of risk response strategies is holistically applied and, where fully justified, cost-effective controls mitigate exposure to risk on a continuing basis. The enterprise formally requires continuous improvement of risk response skills (e.g., risk articulation, mitigation, crisis management) based on clearly defined personal and organisational goals. The enterprise employs advanced risk response technologies to intelligently take on additional risk and seize competitive opportunities.

Early Draft

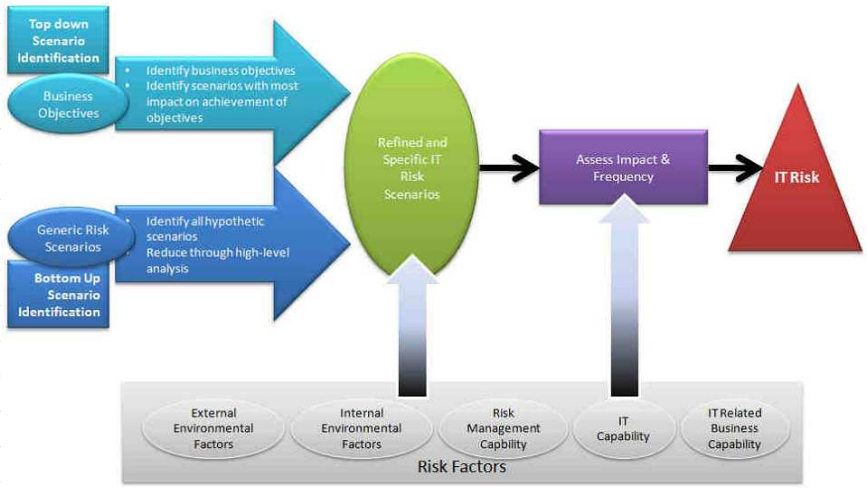
ENTERPRISE RISK: IDENTIFY, GOVERN AND MANAGE IT RISK

The Risk-IT Framework
Practitioners Guide

Table of Contents (draft)

1. Defining a Risk Universe & Scoping Risk Management
2A. Risk Scenarios – Construction
2B. Risk Scenarios – Sample Generic Risk Scenarios
2C. Risk Scenarios –Capability Risk Factors in the Risk Assessment Process (Vulnerabilities, Cause)
2D. Risk Scenarios –Environmental Risk Factors in the Risk Assessment Process
3A. Describing Risk – Expressing impact in business terms
3B. Describing Risk – Qualitative & Quantitative Methods
3C. Describing Risk - Expressing Impact
3D. Describing Risk - Expressing Frequency
3E. Describing Risk – Risk Maps
3F. Describing Risk – COBIT business goals mapping with other Impact Criteria
4. Risk Appetite & Risk Tolerance
5. Risk Response & Prioritisation
6. A Risk Assessment Workflow
7A. Risk Reporting & Communication – Risk Aggregation
7B. Risk Reporting & Communication – Key Risk Indicators & Risk Reporting
7C. Risk Reporting & Communication – Risk Profiles
7D. Risk Reporting & Communication – Risk Awareness and Communication & Information Flows
8. Manage IT Risk using COBIT & Val-IT

2A Risk Scenario Construction



2A (Risk Factors)

2A (Scenarios)

2B Scenario Examples

Description	List of generic IT risk scenarios – this list can be used as a basis to build the organisation's own set of relevant risk scenarios, which in turn will be the basis for their risk management practices.								
Domain	Risk Governance			Risk Evaluation			Risk Response		
Process	RG1	RG2	RG3	RE1	RE2	RE3	RR1	RR2	RR3

30 Scenario Examples

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
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

Scenario Impact

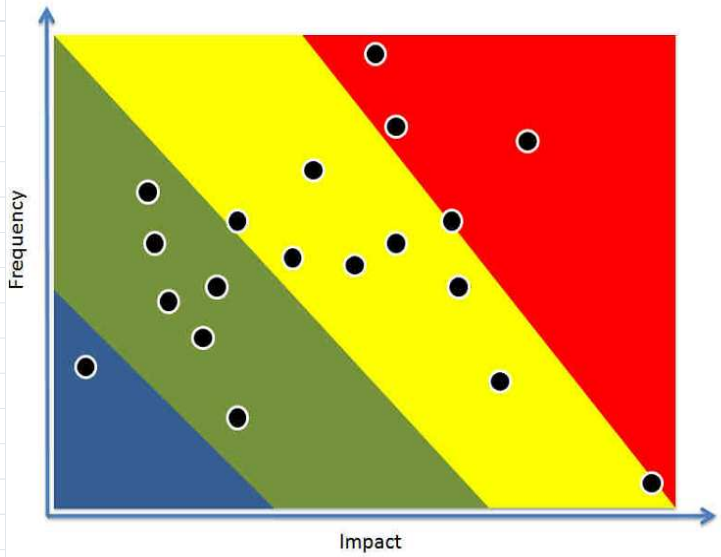
- Systematically work through impact of each scenario on all Cobit and Val IT processes

Generic Scenario	Key Control	Control Reference		Control Title	Control Description	Effect on Impact	Effect on Frequency
IT Project Selection	Yes	PO4	PO4.3	IT Steering Committee	Establish an IT steering committee (or equivalent) composed of executive, business and IT management to: • Determine prioritisation of IT-enabled investment programmes in line with the enterprise's business strategy and priorities • Track status of projects and resolve resource conflict • Monitor service levels and service improvements	Medium	High
IT Project Selection	Yes	AI1	AI1.1	Definition and Maintenance of Business Functional and Technical Requirements	Identify, prioritise, specify and agree on business functional and technical requirements covering the full scope of all initiatives required to achieve the expected outcomes of the IT-enabled investment programme.	Medium	High
IT Project Selection		PM1	PM1.3	Define an appropriate investment mix.	The allocation of funds for IT-enabled investments must be aligned with the strategic direction of the enterprise. The investment mix must achieve the right balance on a number of dimensions which could include, but are not limited to, an appropriate balance of short- and long-term returns, financial and non-financial benefits, and high-risk vs. low-risk investments.	Medium	Medium
					Analyse existing and emerging technologies, and plan which technological direction is appropriate		

Scenario Impact Table

- 35 pages long in preliminary draft
- Provides:
  - Scenario Reference Number & Title
  - Is this Key Control (high impact)
  - Title & Description (from Cobit or Val IT)
  - Estimated effect on impact
  - Estimated effect on frequency

3E Describing Risks – Risk Map



4 Risk appetite & Risk Tolerance

- COSO ERM Definitions
  - **Risk Appetite** – The broad-based amount of risk a company or other entity is willing to accept in pursuit of its mission (or vision).
  - **Risk Tolerance** – The acceptable variation relative to the achievement of an objective (and often is best measured in the same units as those used to measure the related objective)

Key Management Practices RG1

- RG1.3 Perform an enterprise wide IT risk assessment.
  - Sponsor workshops with business management to discuss the broad amount of risk the enterprise is willing to accept in pursuit of its objectives (risk appetite). ...
- RG1.4 Propose IT risk tolerance thresholds.
  - Establish amount of IT-related risk a business, service, process, product, etc., is willing to take. Express limits in measures similar to underlying business objectives and against business impacts. Propose limits over multiple time horizons.
- RG1.5 Approve IT risk tolerance.
  - Evaluate proposed IT risk tolerance thresholds against the enterprise's risk and opportunity levels. Take into account the results of enterprise-wide IT risk assessment. Determine if any unit-specific tolerance thresholds should be applied. Define the types of events and changes that may necessitate a modification to the IT risk tolerance.
- RG1.6 Align policy and standards statements with IT risk tolerance.
  - Perform reviews of IT policies and standards to determine if they reflect the risk appetite and tolerance. If gaps, set target dates, and evaluate against resources required to close the gaps within the proposed timelines. Propose adjustments to risk tolerance levels instead of modifying established and effective operational policy and standards.

7B Key Risk Indicators

- Make a balanced selection of risk indicators, utilising both
  - risk exposures (lag indicators, indicating risk after events have happened) and
  - risk management capabilities (lead indicators, indicating what capabilities are in place to prevent events from occurring).
- Ensure that the selected indicator drills down to the root cause of the events.

7B Selection Criteria

- *Sensitivity* — The indicator must be representative for risk and reliable.
- *Impact* — Indicators for risks with high business impact are more likely to be KRIs.
- *Effort to measure* — For different indicators that are equivalent in sensitivity, the one that is easier to measure is preferred.
- *Reliability* — The indicator must possess a high correlation with the risk and be a good predictor or outcome measure.

Other Standards/Frameworks

Principle/Feature	Risk-IT	COSO ERM	ISO 31000	ISO 27005	AS/NZS4360	ARMS	ISF
Always relate to business objectives							
Align IT Related business risk management with overall enterprise risk management							
Always seek and maintain the balance between Risk and Cost of addressing the IT Related Business Risk							
Provide open and fair communication on IT Related risk							
Establish the right culture at the top and define and enforce accountability for risk management, including personal accountability							
Be a continuous process, where information about IT Related Risk is monitored and updated							
Availability (to the general public)							
Comprehensive view on IT (Related) Risk							

COSO ERM

FOREWORD

"Over a decade ago, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued Internal Control Integrated Framework to help businesses and other entities assess and enhance their internal control systems. That framework has since been incorporated into policy, rule, and regulation, and used by thousands of enterprises to better control their activities in moving toward achievement of their established objectives.

"Recent years have seen heightened concern and focus on risk management, and it became increasingly clear that a need exists for a robust framework to effectively identify, assess, and manage risk. In 2001, COSO initiated a project, and engaged PricewaterhouseCoopers, to develop a framework that would be readily usable by managements to evaluate and improve their organizations enterprise risk management."

ISO/FDIS 31000: Risk management

"ISO 31000:2009 provides principles and generic guidelines on risk management.
"ISO 31000:2009 can be used by any public, private or community enterprise, association, group or individual. Therefore, ISO 31000:2009 is not specific to any industry or sector.
"ISO 31000:2009 can be applied throughout the life of an organization, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets.
"ISO 31000:2009 can be applied to any type of risk, whatever its nature, whether having positive or negative consequences."

- 24 pages – from AS/NZS 4360:200

ISO/IEC 27005:2008 Information security risk management

"ISO/IEC 27005:2008 provides guidelines for information security risk management. It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach. Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of ISO/IEC 27005:2008. ISO/IEC 27005:2008 is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that could compromise the organization's information security."

ARMS: Airline Risk Management Working Group

"The Mission of the ARMS Working Group is to produce useful and cohesive Operational Risk Assessment methods for airlines and other aviation organisations and to clarify the related Risk Management processes.

"The produced methods need to match the needs of users across the aviation domain in terms of integrity of results and simplicity of use; and thereby effectively support the important role that Risk Management has in Aviation Safety Management Systems."

ISF: Information Security Forum

"The Standard of Good Practice for Information Security (the Standard) is the foremost authority on information security. It addresses information security from a business perspective, providing a practical basis for assessing an organisation's information security arrangements.

"The Standard represents part of the ISF's information risk management suite of products and is based on a wealth of material, in-depth research, and the extensive knowledge and practical experience of ISF Members worldwide."

Concern

- External view of risk
  - Start with a project or process
  - Assess the risks faced by the project or process
  - Develop appropriate tactics and strategies
- Internal view of risk
  - Use risk to help define project or process
  - Assess the remaining risks
  - Review the definition in light of risks
  - Develop appropriate tactics and strategies

Pretty Picture, but ...

- Cruel illusion to pretend that projects never need to revisit past decisions

Personal Hobby Horse

- Waterfall was never very good
- Waterfall, today, works less well
- Something different needed
- Boehm's Spiral
- DoD requirement
- Interesting to apply to outsourcing

Waterfall Life Cycle Model

- Requirement are pre-specifiable
- Requirements are slowly changing
- Requirements good for all stakeholders
- Requirements can be met using well understood architecture

  - No Uncertainty Principle

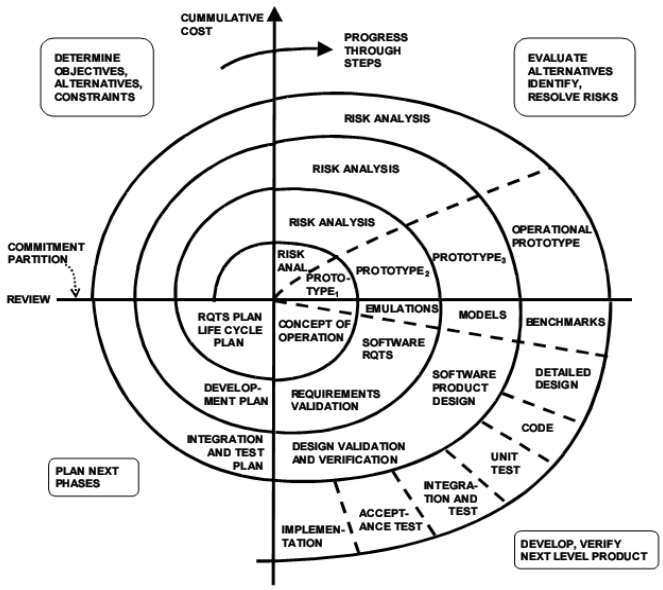
Uncertainty Principle for Systems

- Actual experience with a system changes our understanding of the system requirements

Uncertainty Principle
"The more precisely the POSITION is determined,
the less precisely the MOMENTUM is known"

W. Heisenberg

Spiral System Life Cycle



In Boehm's Words

- The spiral development model is a *risk* driven *process model* generator that is used to guide multi-stakeholder concurrent engineering of software-intensive systems. It has two main distinguishing features. One is a *cyclic* approach for incrementally growing a system's degree of definition and implementation while decreasing its degree of risk. The other is a set of *anchor point milestones* for ensuring stakeholder commitment to feasible and mutually satisfactory system solutions.

Spiral Options

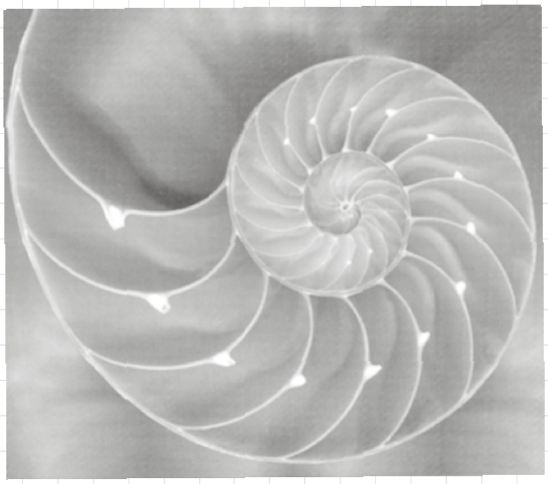
- No requirement to conduct more than one cycle (risk driven)
- Even performing two cycles can be a great simplifier

- US DoD: "software development and acquisition ***shall*** follow an iterative spiral development process"

Outsourcing Acquisition Risk

- There are important differences
  - Buying a ton of sand
  - Buying an IT outsourcing contract
- In IT, it's buying a process
- Waterfall works for buying sand
- Waterfall doesn't work for buying outsourcing

IT Outsourcing Spiral



High reward, high risk

Outsourcing Results

- 67% wanted outsourcing to reduce costs; 74% achieved that
- 48% wanted outsourcing to improve processes; 65% achieved that
- 35% wanted outsourcing to let them focus on core business; 75% achieved that
- 61%: Outsourcing has helped my company perform better

Accenture Executive Survey

Restated

- 29% failed to achieve desired cost reduction
- 35% failed to adequately improve processes
- 25% failed to improve core business focus

- 39%: Outsourcing has not helped my company perform better

Challenges

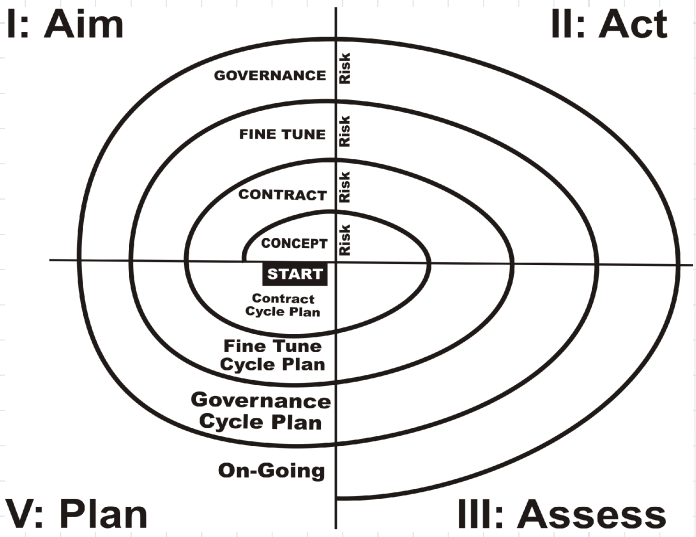
- Outsourcer not performing to expectations
  - Best in class: 40%; All: 51%
- Don't have right skills/staff to manage
  - Best in class: 33%; All: 42%
- Too much executive time required
  - Best in class: 47%; All: 33%
- Didn't get planned cost reductions
  - Best in class: 20%; All: 28%

Outsourcing

- Responsible management can't ignore outsourcing – too many reported benefits
- But there are serious risks – many failed to achieve expected results
- Failure can be painful – contract can become a business straight-jacket

Trust me, it's a great contract!

IT Outsourcing Spiral



Spiral Quadrants

- AIM
  - Establish/Confirm cycle target
- [RISK]
  - [Risk drives detail and depth]
- ACT
  - Carry out the work of this cycle
- ASSESS
  - Evaluate/Assess the work, possible stop
- PLAN
  - Plan for next cycle

Spiral Cycles

- Concept
  - Is there an attractive win-win concept?
- Contract
  - Select a vendor and translate from concept to contract
- Fine Tune
  - Install the service and tune it to meet local experience
- Governance
  - Put in place on-going, effective governance

Outsourcing Advantages

- Economies of Scale
- Access to Technology
- Access to the right People
- Simplified Compliance
- Attractive Financial deal
- Etc., etc., etc.

Disadvantages

- The vendor needs to make a profit
- Negotiating with experienced suppliers
- Not a "real" partnership
- Must lock-in services for 3 - 7 years
- Radical change is hard to achieve
- Oversight responsibilities remain

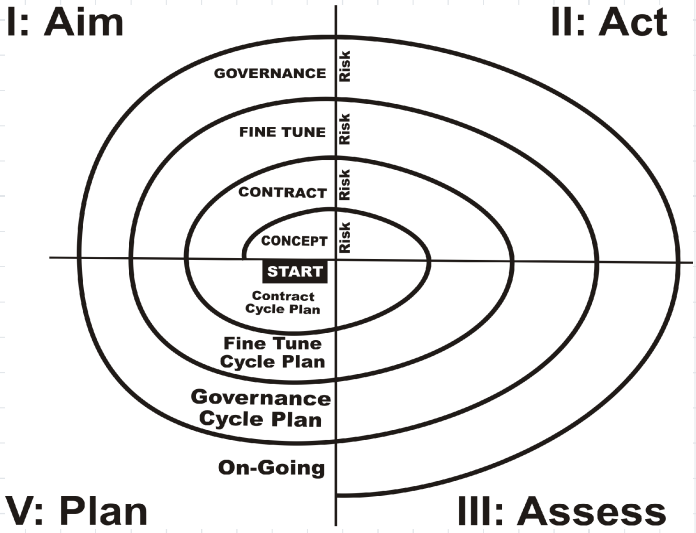
Problems

- Service bureau game
  - Profit comes from all of the extras
- Conditions change
  - Company changes, markets change, ...
- Only initial advantage
  - Gets painful if advantage doesn't continue
- No management direction
  - You get the consultant you deserve/expect

Avoid being sucked in ...

- "A" team, replaced by ...
- "B" team, replaced by ...
- "C" team, replaced by ...
  - *agh, ... dragged under!*

IT Outsourcing Spiral



Concept Cycle

- AIM: Identify attractive win-win concepts
- RISK: People, sub-optimal, missed concept
- ACT: Invention, then Market Probe
- ASSESS: Win-win today & tomorrow
- PLAN: Best path to a contract

Make it a Win-Win!

Unobtanium

- The vendor must add something that would be unobtainable by the client
- In the absence of *unobtanium,* the deal will not make sense
  - The vendor must take its profit off the table
  - The client expects that costs will not rise
  - Unobtanium - "magic sauce" making it work

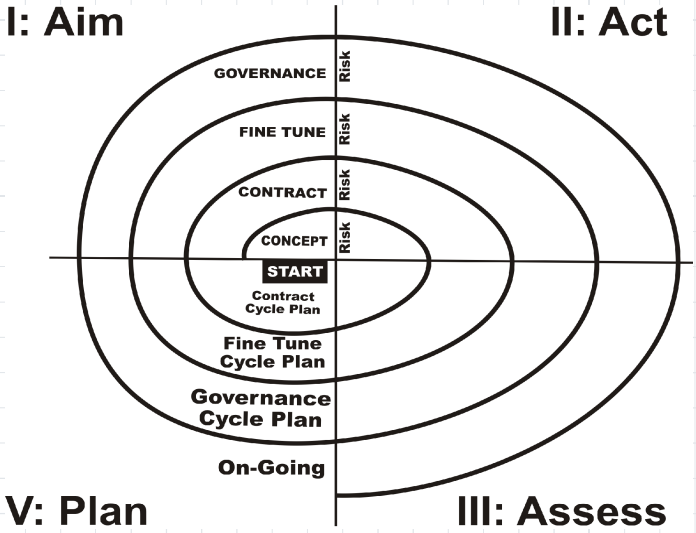
Core Competency

- Don't outsource something that is core to your business
  - Few IT services are really core to the business
- Target buying from the outsourcer's core competency
  - Risk increases if concept critically depends on things outside the vendor's demonstrated core competency

Exceptions

- Extending a successful contract
  - Same cycles, but much simpler
- Finding alternatives to failing contract
  - Still need alternative concept(s)
- A way to achieve organizational change
  - Limited life time of concept value
- Real partnership with vendor
  - Beware vendor marketing hype

IT Outsourcing Spiral



Contract Cycle

- AIM: Translate from concept to contract
- RISK: People, wrong vendor, wrong contract
- ACT: Multiple parts -
  - Acceptable vendors
  - Responsive offers
  - Verification/validation
  - Negotiation
- ASSESS: What's critical to implementation
- PLAN: Transition to Fine Tuning

Alternatives

- Separate RFI Cycle
  - Yes if it's big and public
- Separate Concern Cycle
  - Short-list based on response to concerns
- Multiple Phases
  - May be required if multiple physical sites
- Caution
  - Don't let it drag out too many years

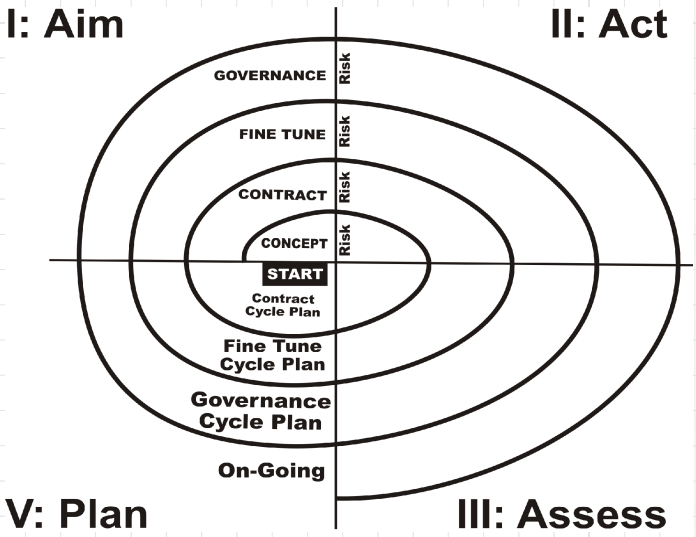
Verification/Validation

- Vendors will tell you what they think you want to hear
- Test claims
  - Maturity level
  - Bench strengh
  - Customer satisfaction
- Consider actual tests

Contract Observations

- Build the concept into the contract
  - Measure and recognize concept delivery
- Be flexible in your service demands
  - Benchmarking is an odd "science"
- Don't allow hopeless conditions to arise
  - People always need to see a way to win
- Limited, flexible measures
  - Measure key variables, allow them to change

IT Outsourcing Spiral



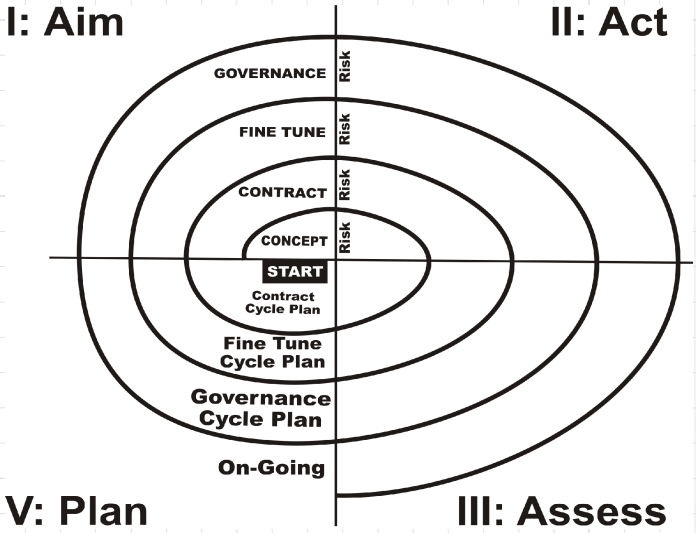
Fine Tune Cycle

- AIM: Translate into practice, adjust
- RISK: People, too much, too little
- ACT: Roll out, operate, adjust
- ASSESS: Anything special required
  - Don't let problems fester
- PLAN: What's required to govern

Governance Cycle

- AIM: Smooth operation
  - Achieve level 3+ maturity?
- RISK: People, inappropriate measures
- ACT: At least one full cycle
  - Reports must be read, meeting must happen
  - Not just once, but on a regular basis
- ASSESS: When do we need to begin again

IT Outsourcing Spiral



This Session

- Professional Risk Responsibility
- Corporate Risk Responsibility
  - Either ERM or GRC
- COBIT view of IT Risk
- Risk IT
  - Framework
  - Sampled Details
- Risk Oriented Spiral

Tomorrow

- So IT Risk is important …
  - So what?
    - What will be different tomorrow?
    - What will you start / stop doing?
    - How should risk change planning?

Literature Pointers

- *A Risk Management Standard*, a high level, UK standard, 2002 (free)
- *Enterprise Risk Management – Integrated Framework*, Treadway Commission (COSO), 2004
- *Risk Management: Guideline for Decision-Makers*, CAN/CSA-Q850-97, 1997
- *CobiT*, version 4.1, IT Governance Institute, 2007 (free)

Literature Pointers – II

- *CrossTalk*, The Journal of Defense Software Engineering, February 2005 (free)
- *Guidelines for Successful Acquisition and Management of Software-Intensive Systems*, US Air Force Software Technology Support Center, Version 3.0 (2000, full) and Version 4.0 (2003, condensed) (free)
- *IEEE Standard for Software Life Cycle Processes – Risk Management*, 1540-2001

Literature Pointers – III

- *The Risk IT Framework,* Exposure Draft, ITGI, February 2009 (free)
- *Taxonomy-Based Risk Identification*, CMU/SEI-93-TR-6, June 1993 (free)
- *Software Risk Management*, CMU/SEI-96-TR-012, June 1996 (free)
- *A Taxonomy of Operational Risks*, CMU/SEI-2005-TN-036, 2005 (free)

Literature Pointers – IV

- *A Guide to the Project Management Body of Knowledge*, 2008 version, Project Management Institute
- *Information technology – Code of practice for information security management*, ISO/IEC 17799:2001
- *Software Assurance – A Curriculum Guide to the Common Body of Knowledge to Produce, Acquire, and Sustain Secure Software*, US Homeland Security (2007) (free)

Literature Pointers - V

- *Spiral Development: Experience, Principles, and Refinements,* February, 2000, CMU/SEI-2000-SR-008 (free)
- *ISO/FDIS 31000 Risk management -- Principles and guidelines*, final draft, (downloaded 2009.10.13)
- *CIPS Risk Management Practice Framework*, CIPS, 2007 (free)
- *Background: CIPS Risk Management Practice Framework*, rfabian.com/risk (free)