The Greater Kansas City ISACA Chapter

protiviti[SM]
Independent Risk Consulting

An Enterprise Approach to Information Technology Risk Analysis

Tom Andreesen – Protiviti

January 13, 2005

Business Risk | Technology Risk | Internal Audit

Discussion Topics

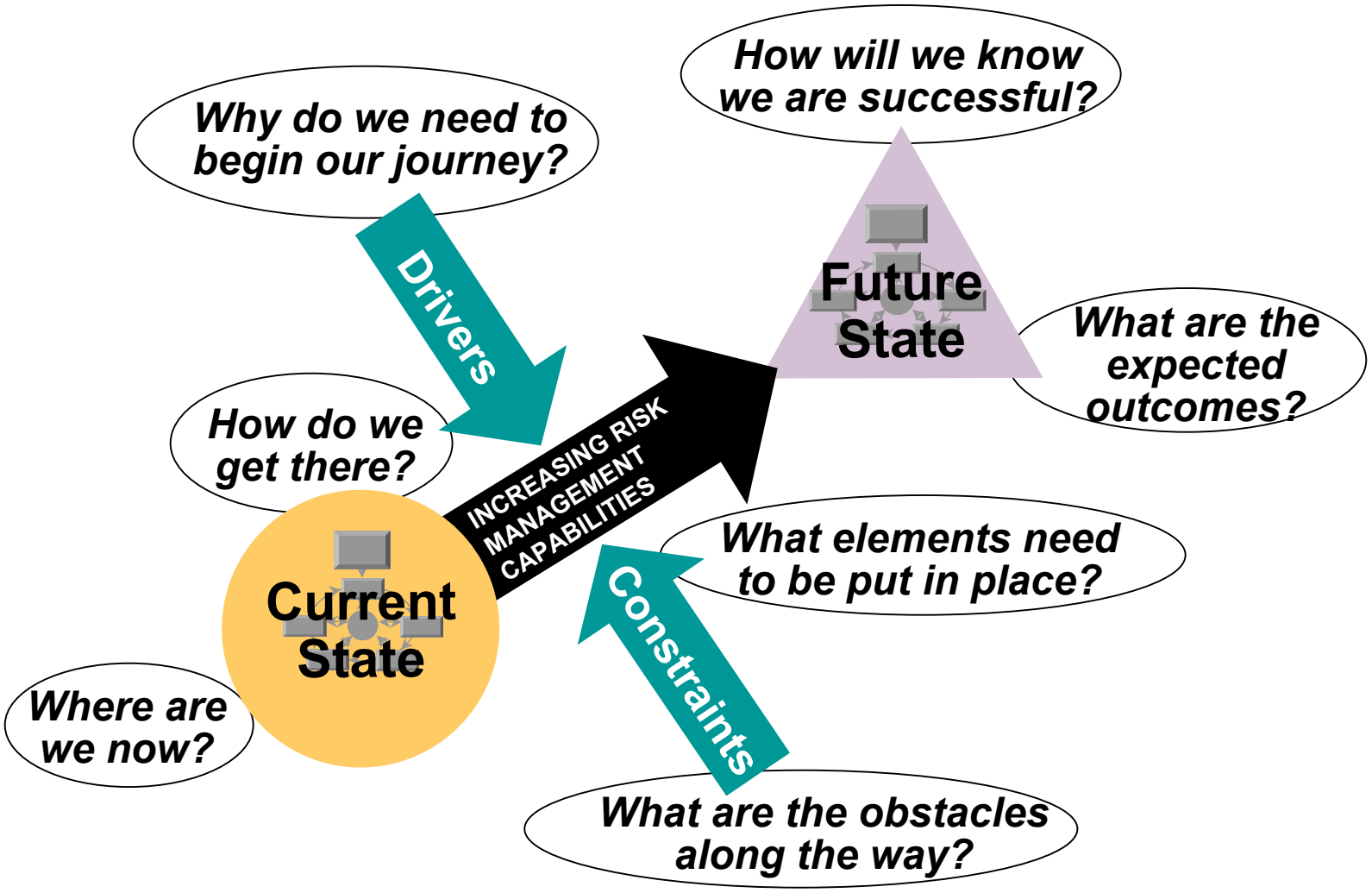
- Enterprise Risk Management Level Setting
- State of Technology Risks
- Expand Technology Horizons
- Measuring the Technology Risks
- Value Proposition
- Getting Off the Starting Line
- Questions

Enterprise Risk Management Level Setting

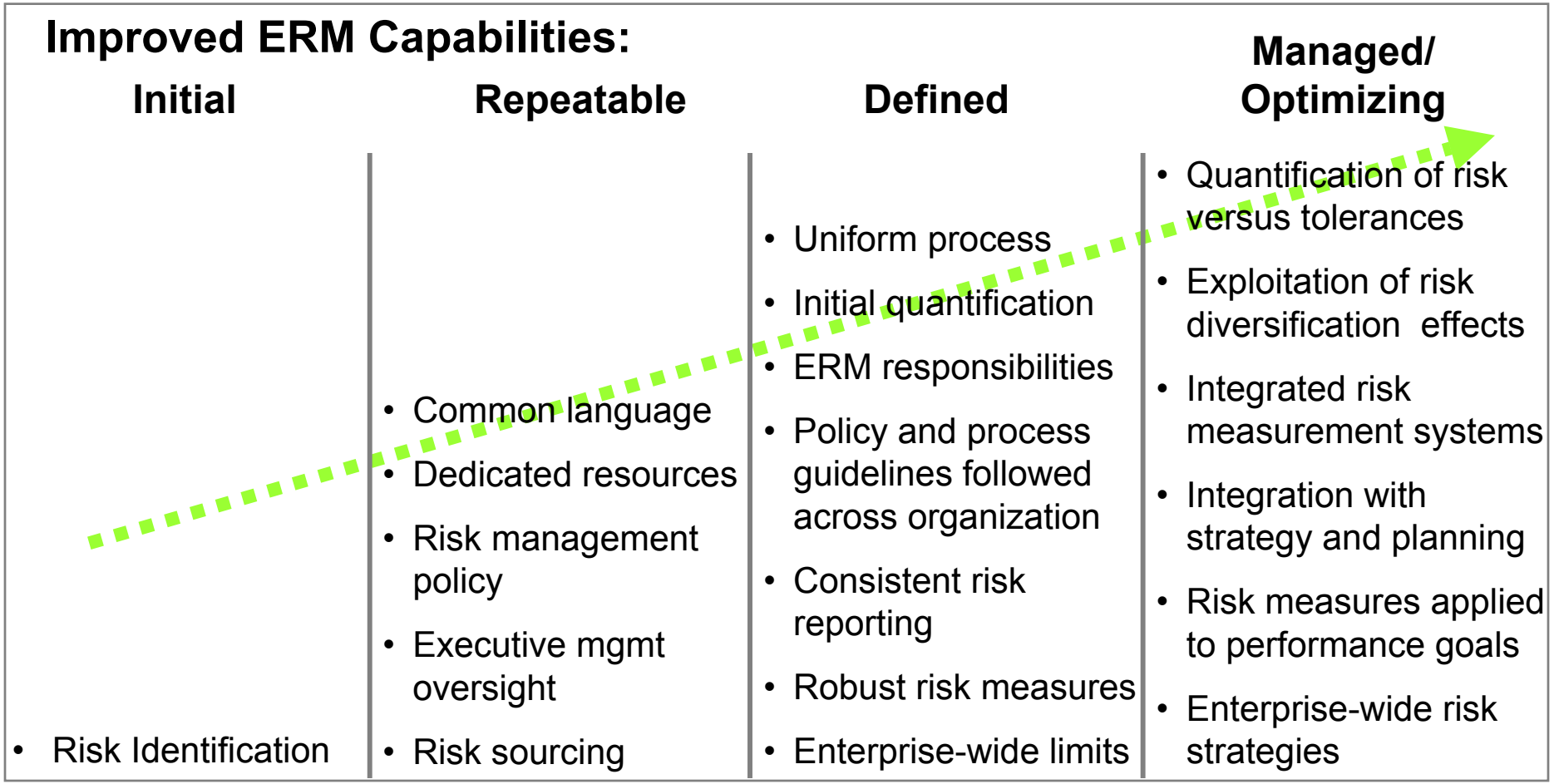
Enterprise Risk Management Defined

Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its appetite, to provide reasonable assurance regarding the achievement of entity objectives.

ERM is a Journey not a Destination and Requires a Change Process



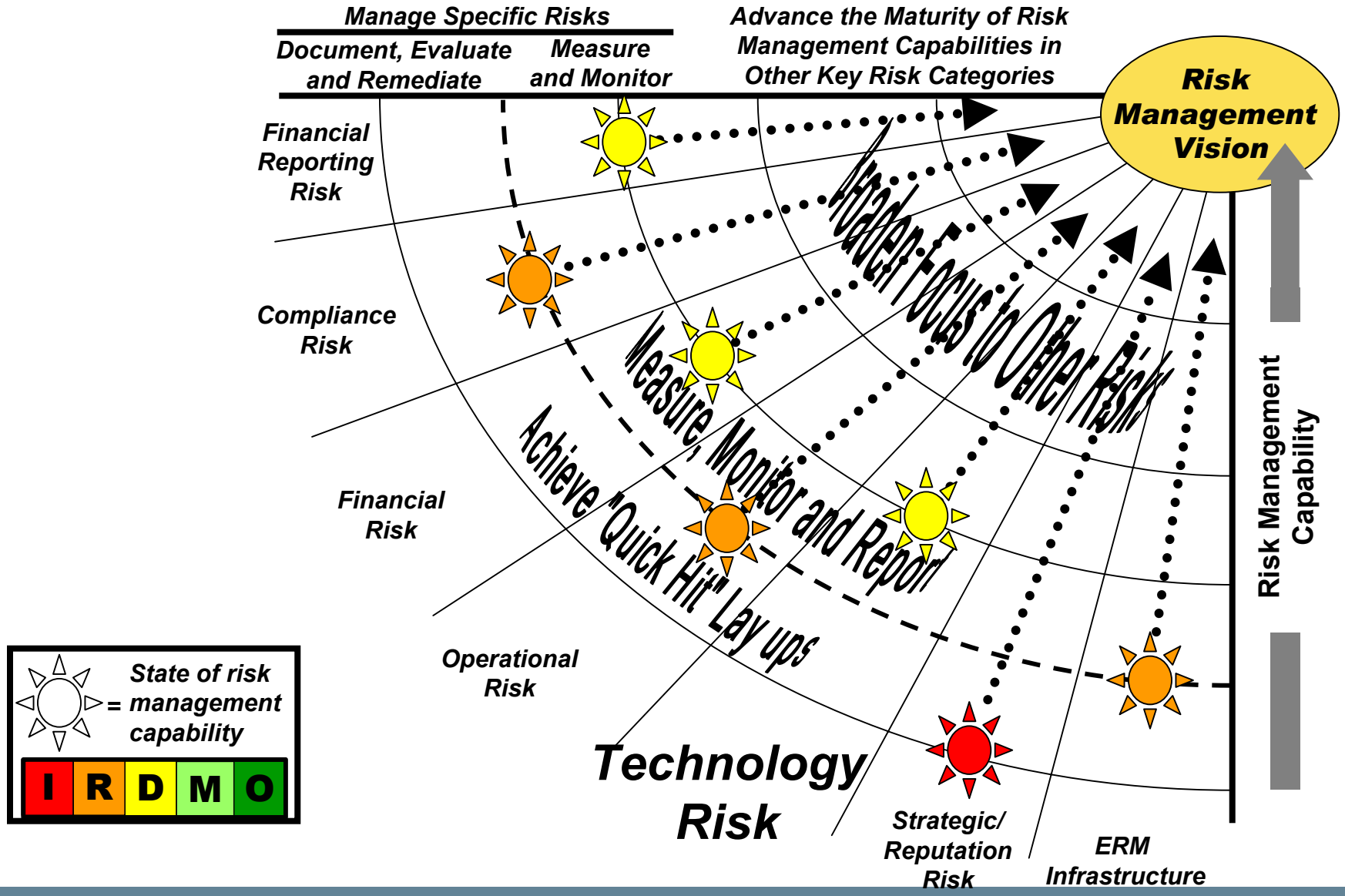
ERM is a Growth Process Consisting of Specific Steps to Improve Risk Management Capability



Examples of Foundation Elements

	Adopt common language	***Establish oversight and governance***
Does the company have:	A common language for risks and risk management?	Overall an effective oversight structure and governance?
Possible Journey elements	• Risk model • Risk management glossary • Process classification scheme • Other relevant frameworks • Improved dialogue about risk and its sources, drivers or root causes • More organized process for sharing of information	• Overall risk management policy • Top-down communications of risk management direction • Organizational oversight structure, with Board oversight • Risk management oversight committee(s) and management accountability • Designated senior executive responsible for risk management (I.e., a CRO) • Risk management and governance processes integrated • Business risk management staff function
Possible expected outcomes	• Increase chances of identifying all key risks • Enable people from multiple disciplines to focus on issues faster	• Achieve clarity as to risk management role, purpose and accountabilities • Get things done quicker by executives empowered to act

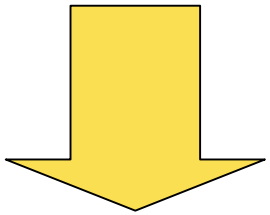
Broadening the Risk Coverage



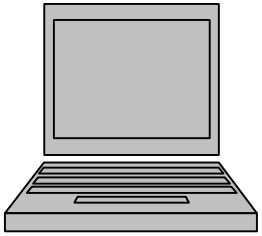
State of Technology Risks

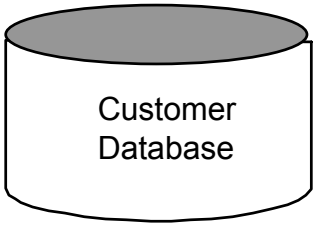
Enterprise Risk Management Defined

Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its appetite, to provide reasonable assurance regarding the achievement of entity objectives.



BUT DO THESE PERSONNEL REALLY THINK ABOUT THESE….



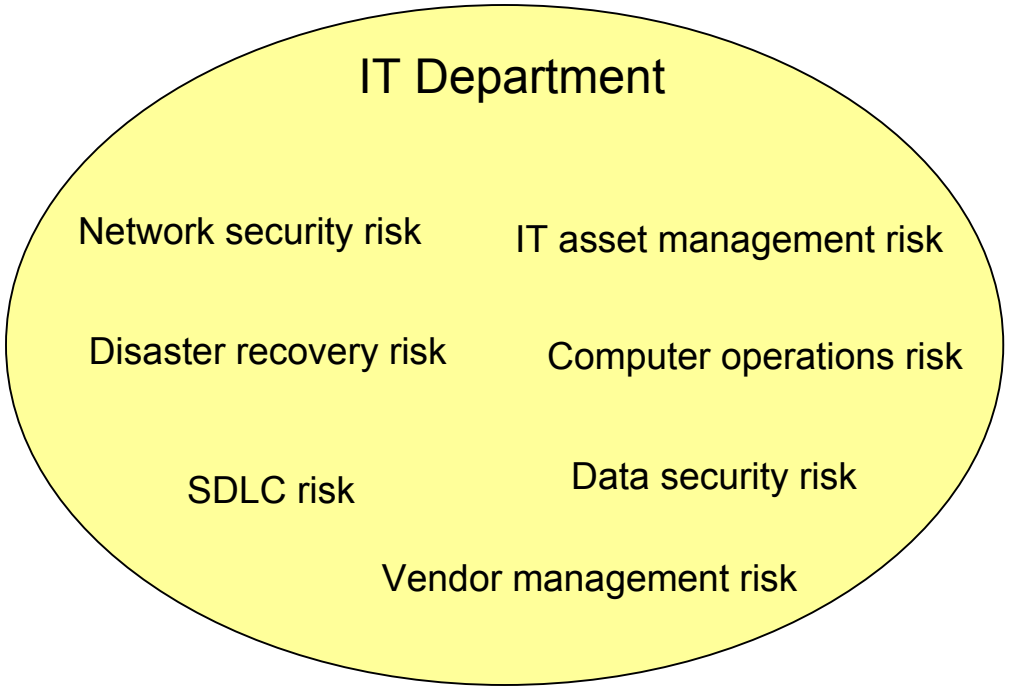


Enterprise Risk Management - Key Indicators of Need

- Management wants increased confidence that all potentially significant information technology (IT) risks are identified and managed besides those that have financial reporting risk impact
- Key decisions are made without a systematic evaluation of risk and reward trade-offs
- No clearly articulated IT enterprise-wide strategies for taking and bearing risk
- IT risk management isn't integrated with strategic and business planning
- IT risks are not systematically identified, sourced, measured and managed on an aggregated basis
- Units of the organization are managing similar IT risks differently
- Increasing demands for more information relating to IT risks and internal controls from the board and investors
- Key IT functions and infrastructure are outsourced to a third party

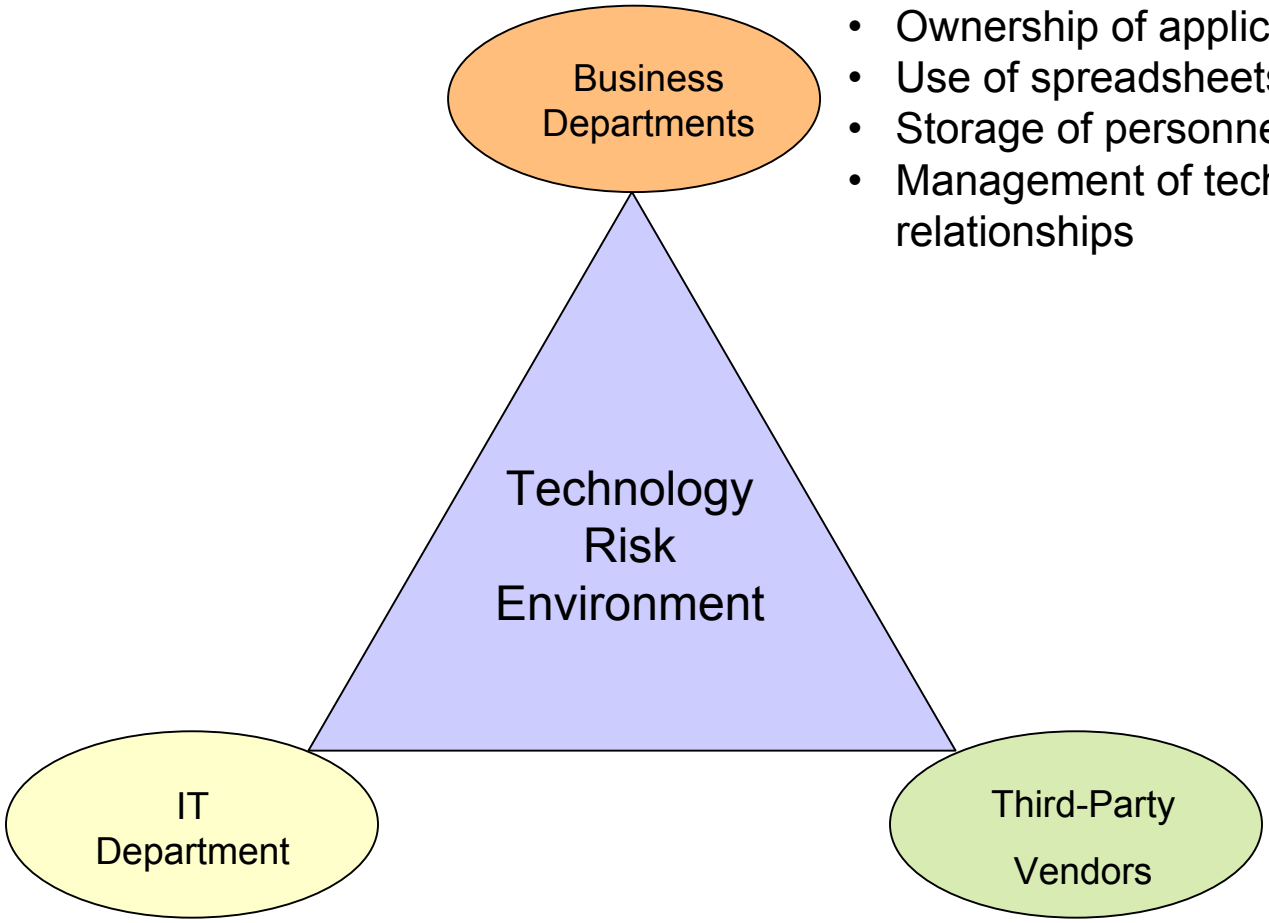
Identifying the Technology Risks

Typical assessments pinpoint risks to be rooted in the Information Technology (IT) department.



Identifying Technology Risks

Compliance work has illustrated that technology risks are in unexpected places.

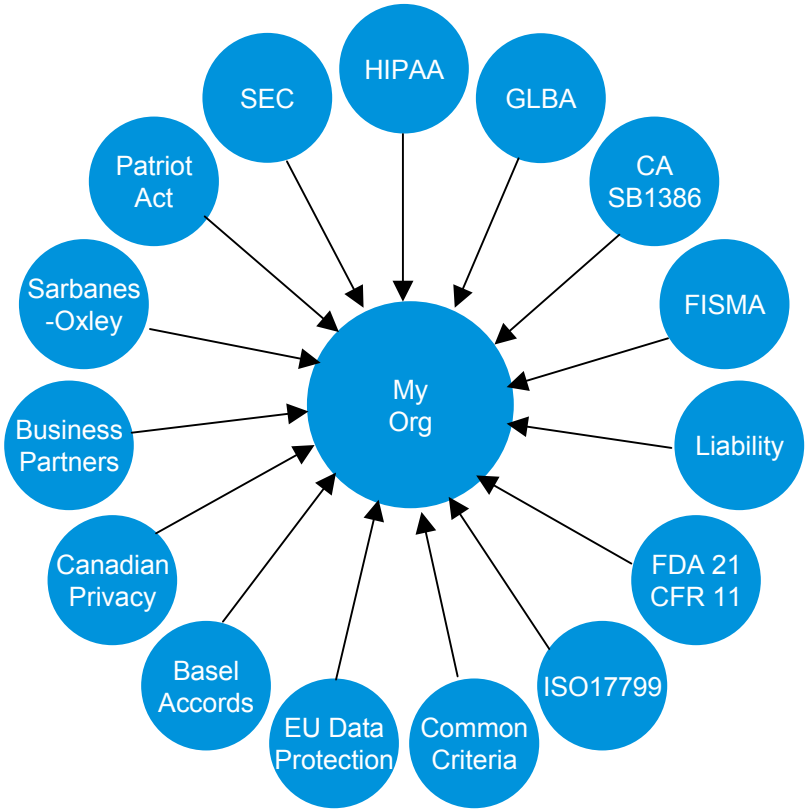


- Ownership of applications
- Use of spreadsheets
- Storage of personnel medical information
- Management of technology vendor relationships

- Key transaction processing
- Storage of customer information
- Lack of any SAS70-type of review

The Regulatory Environment Adds Complications

Example of regulatory impact from a security perspective – not a pretty picture.



Source: Giga Information Group, Inc.

The Typical Approach is NOT EFFECTIVE

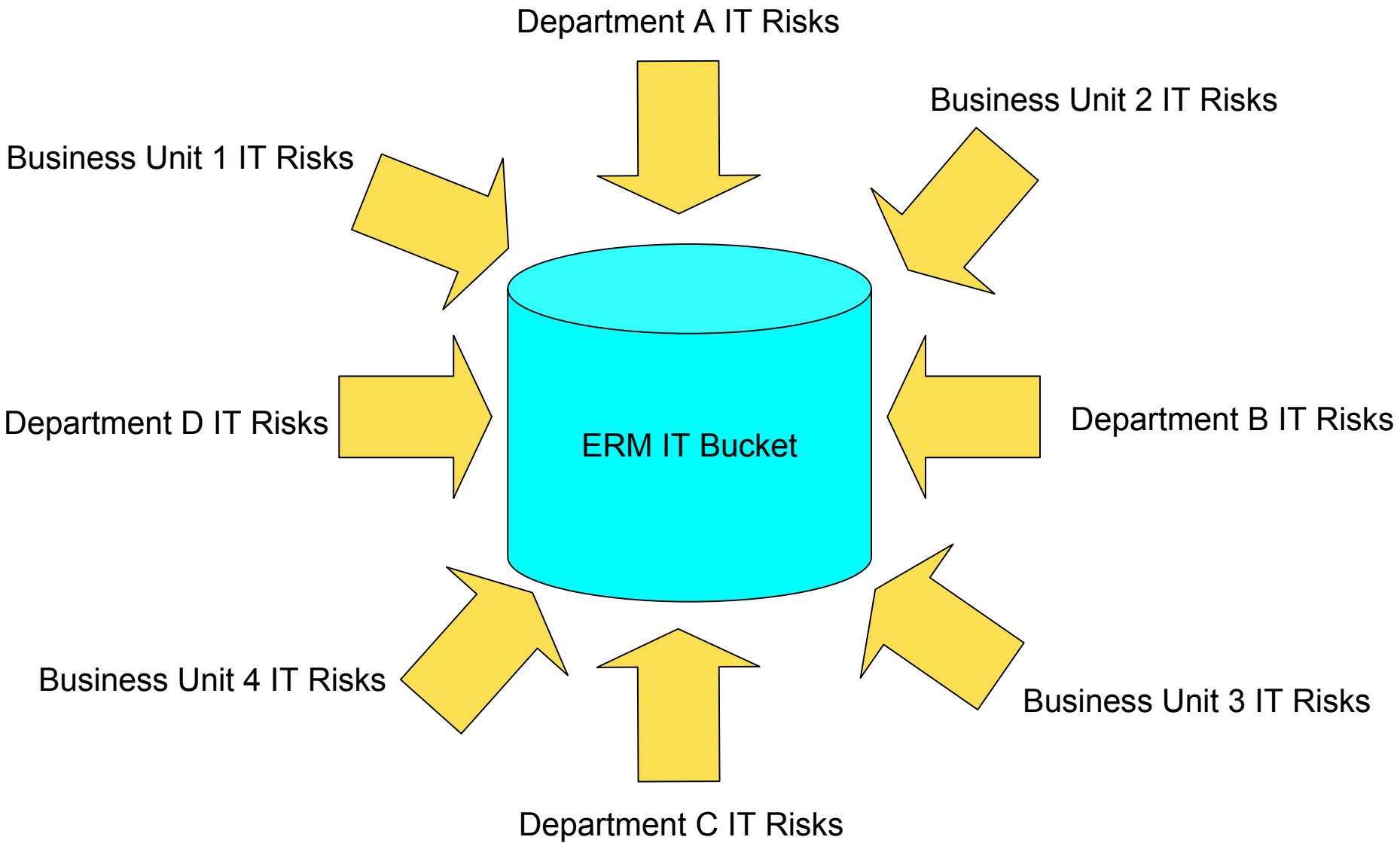
MR. DEPARTMENT HEAD, ANYTHING CHANGED IN THE BUSINESS THAT HAS TECHNOLOGY IMPACT?

MS. DEPARTMENT HEAD, IS THE IT GROUP SUPPORTING YOU WELL ENOUGH?

MS. DEPARTMENT HEAD, ANY TECHNOLGY RISKS THAT YOU KNOW ABOUT?

MR. DEPARTMENT HEAD, WHAT KEEPS YOU UP AT NIGHT?

We Need to Develop our Enterprise View



Expanding Technology Horizons

IT Risk Assessment

The risk assessment process detailed below outlines the strategy, execution, and support necessary to implement a defined, effective, and repeatable approach to addressing IT risk.

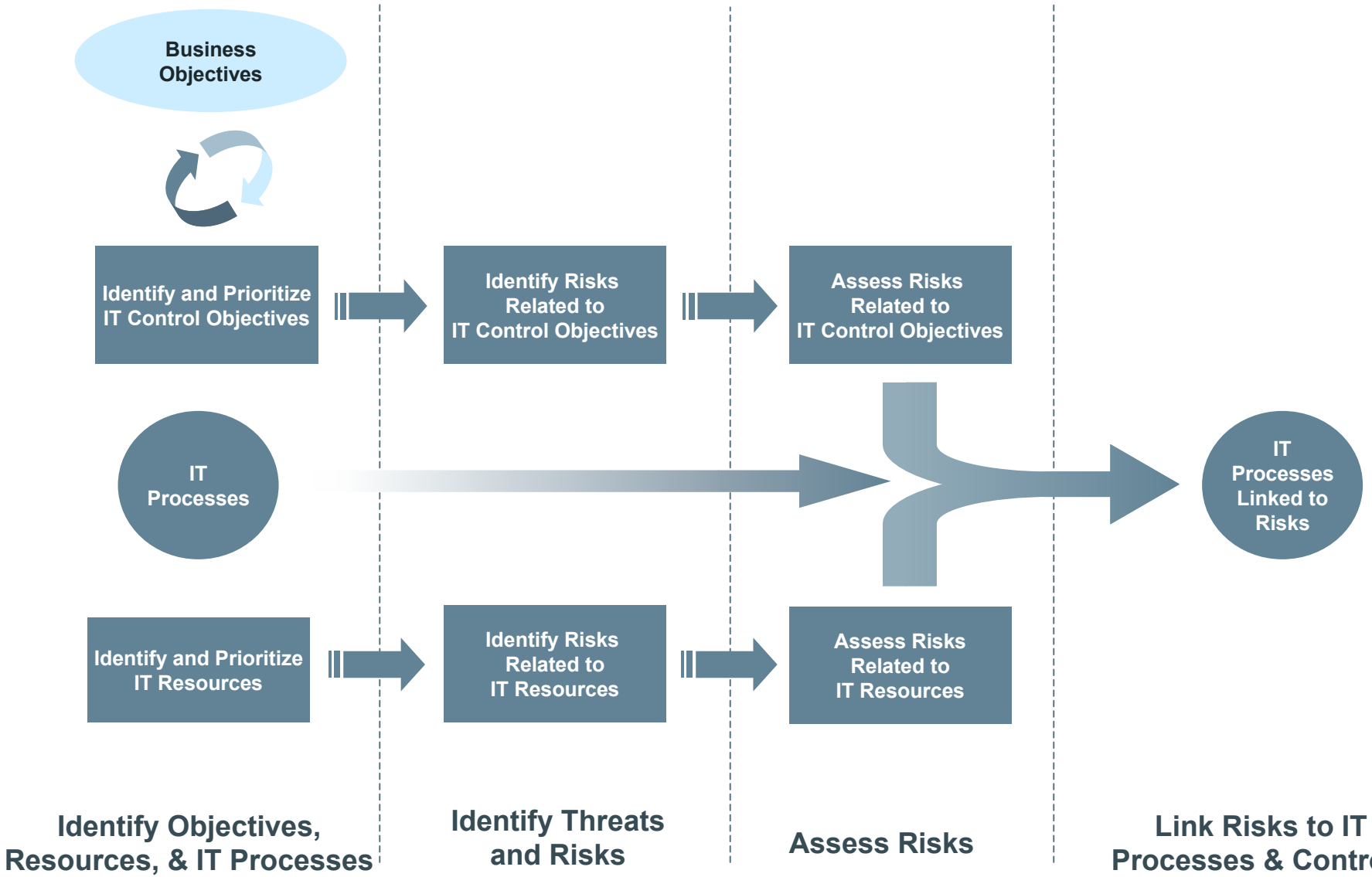
Risk Assessment Process

IT Risk Assessment - Strategy

Definition of an Organizational Risk Management Strategy helps ensure global awareness of IT governance issues. An effective Risk Management Strategy includes:

- Integration into enterprise risk management process
- Establishment of an IT risk management oversight board with executive sponsorship
- Identification of necessary skill sets to perform an effective and comprehensive IT risk assessment
- Definition of risk management activities that have a clear purpose, are documented and implemented based on enterprise IT needs.
- Development of a defined risk assessment framework to base risk management activities on. Risk assessment framework should include definition of common terms and language
- Execution of risk assessments on a regular basis at both an enterprise level and more detailed project or risk specific level
- Development of a standard set of metrics to measure risk assessment process and results.

IT Risk Assessment - Methodology



IT Risk Assessment - Methodology

Identify Objectives, Resources, & IT Processes

- Identify IT objectives based on a defined framework (maybe COBiT)
- Identify IT Resources including, technology, data, people,
- Use survey or affiliated session to prioritize identified IT objectives and IT resources
- Identify core IT processes and controls supporting the business

Identify Risks & Assess Risks

- Develop preliminary listing of risks for IT objectives and resources
- Use facilitated sessions with senior IT management to identify risks related to IT Objectives
- Use facilitated sessions and interviews with key IT personnel to identify risks related to IT resources
- Assess identified risks based on significance and likelihood

Link Risks to IT Processes & Controls

- Determine risk mitigation strategy based on risk assessment levels
- Link risks to identified IT processes and controls
- Identify residual risks (gaps)

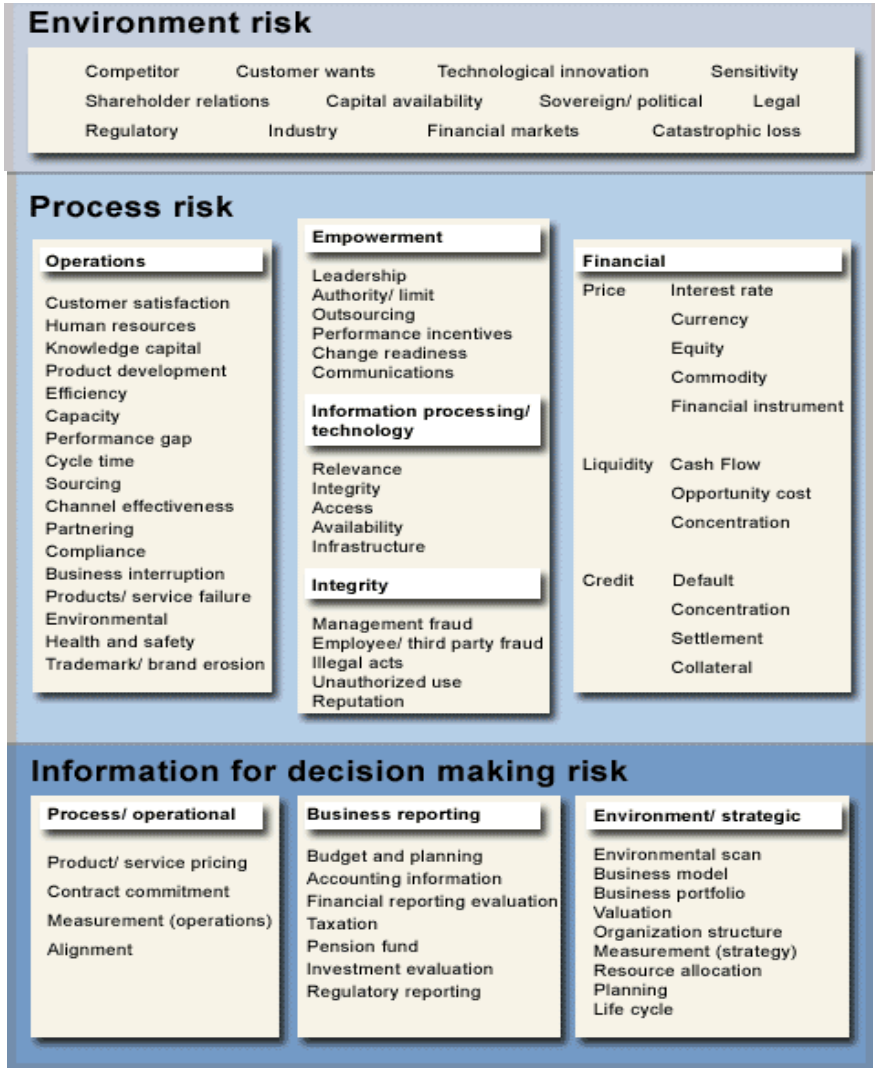
IT Risk Assessment - Foundation

Building a risk management process on a solid foundation helps ensure an efficient and effective process that is flexible enough to be leveraged across the organization and adapt to changing business or IT objectives and risks. An effective foundation consists of the following:

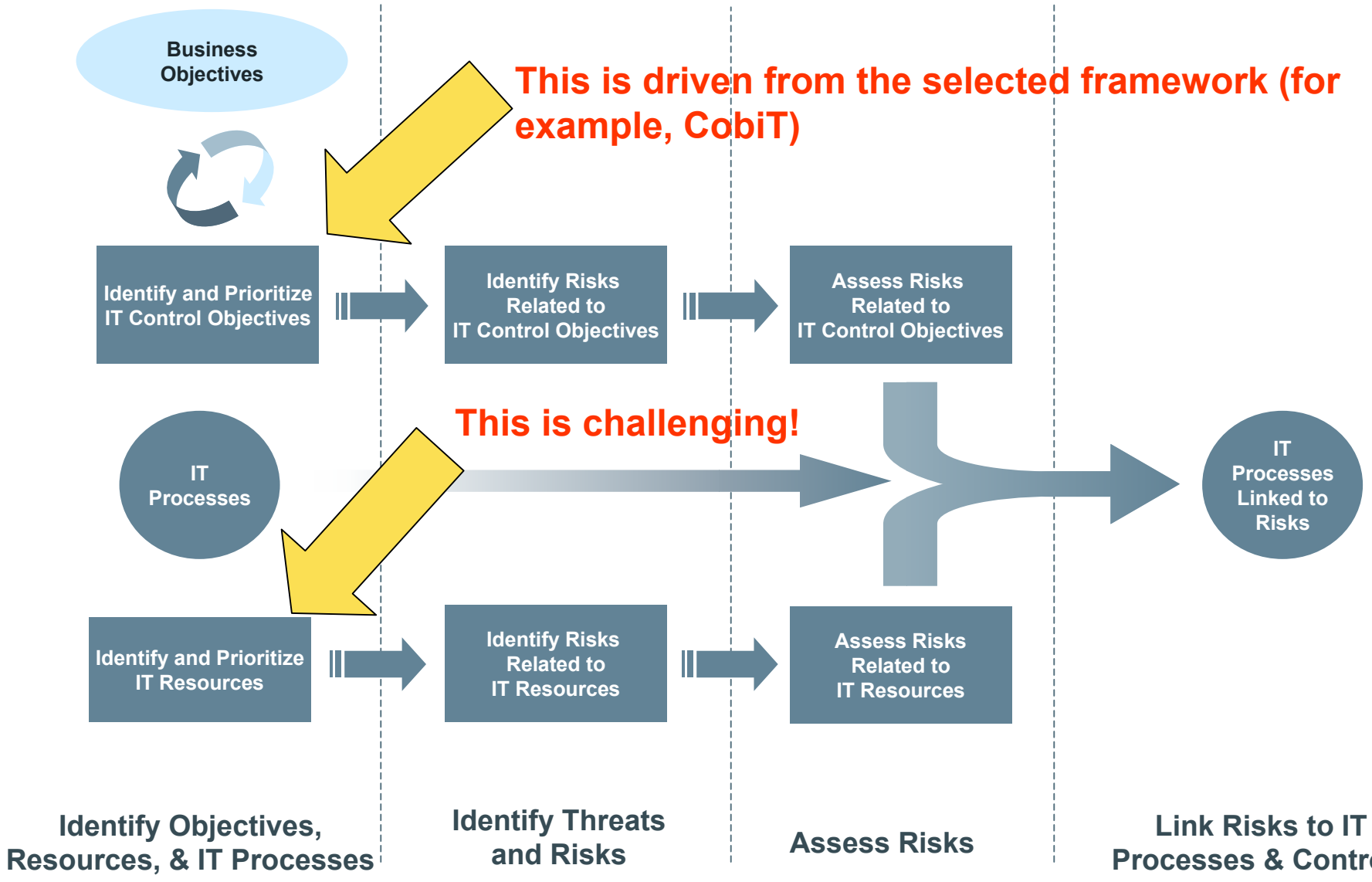
- Documentation of risk management process, framework, policies, and procedures
- Identification of specific risk management resources including, technology and people
- Commitment by personnel to integrate the risk management process into other enterprise risk management efforts
- A mechanism to measure and continuously improve the process maturity

Establishing the Common Language

The ERM efforts within the company have likely generated a model that provide the basis for speaking the same language and building the IT risk framework.

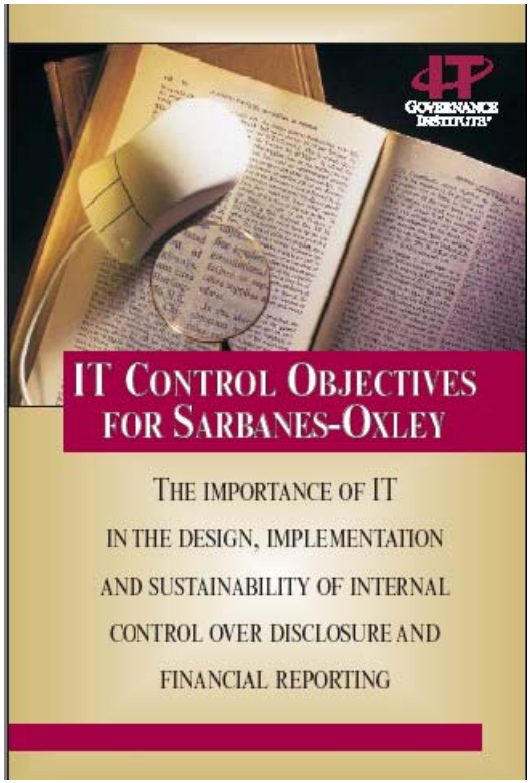


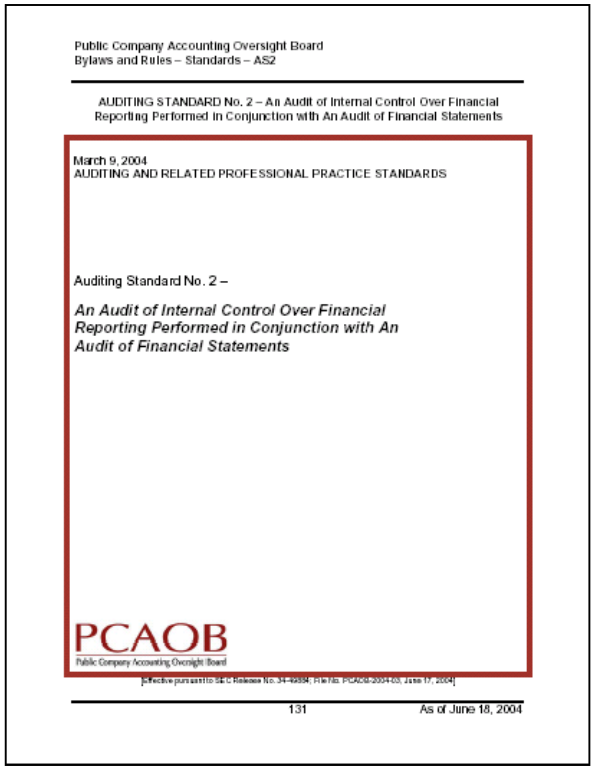
IT Risk Assessment - Methodology



Identifying IT Control Objectives

Public companies already have a great start on their objectives. Now, they may need to be expanded to account for non-financial reporting related elements.




Public Company Accounting Oversight Board
Bylaws and Rules – Standards – AS2

AUDITING STANDARD No. 2 – An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements

March 9, 2004
AUDITING AND RELATED PROFESSIONAL PRACTICE STANDARDS

Auditing Standard No. 2 –

An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements

PCAOB
Public Company Accounting Oversight Board

131 As of June 18, 2004

Identifying IT Resources

An approach is to utilize the ERM results for business processes and drive to the application level. Ownership is essential to establishing potential gaps in managing the risks.

Application Owner:	Person 1	Person 2	Person 2	Person 1	Person 1
	Application A	Application B	Application C	Application D	Application E
Business Process1	x		x		x
Business Process2		x	x	x	
Business Process3	x	x	x	x	x
Business Process4				x	

Person 1: IT application director

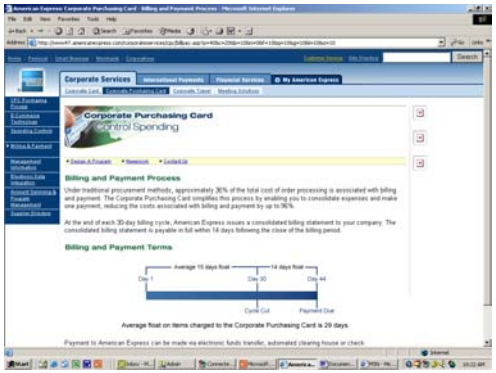
Person 2: Business department director

Identifying IT Resources (cont.)

Applications can take many forms. Beware of interpretations!

Excel Application

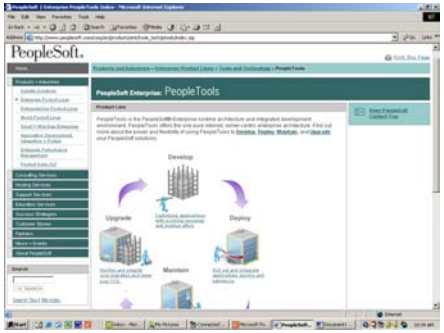
TXN ID	Script	No Volume	Win 1 Base	Win 1	Win 2 Base	Win 2	Win 3 Base	Win 3	Win 4 Base	Win 4 Base 2
AP1R1	voucher_entry						4.40	6.28	5.79	6.25
AP1R2	voucher_entry						3.62	5.23	5.67	4.95
AP1U1	voucher_entry						4.44	5.26	6.74	6.64
GL1IR1	check_journal_status	0.01	0.61	1.34	1.16	1.88	1.20	1.16	2.14	1.86
GL7R1	journal_inquiry	2.25	2.05	4.64	1.16	4.80	3.77	15.30	4.44	2.02
GL7U1	journal_inquiry	2.93	0.13	0.11	0.11	0.22	0.06	0.16	0.09	0.11
AP2R1	voucher_template_entry	1.73					4.58	5.21	8.66	6.34
AP2U1	voucher_template_entry	4.84					3.39	4.44	5.90	4.33
AP12R1	voucher_status	1.15	1.2	1.42	0.76	2.20	1.97	1.39	1.63	1.26
AM1R1	asset_express_add									
AM1U1	asset_express_add	4.93								
AM4R1	asset_retire_full	2.97								
AM4U1	asset_retire_full	3.58								
AM2R1	asset_basic_add									
AM2R2	asset_basic_add	3.44								
AM2U1	asset_basic_add	8.62								
AP4R1	vendor_update		3.06	29.19	3.16	3.89	4.16	4.84	4.22	4.55
AP4U1	vendor_update	0.35	0.2	0.19	0.19	0.17	0.16	0.14	0.16	0.17
GL14R1	ledger inquiry		4.94	5.16	3.34	6.36	6.84	7.28	12.61	8.69
GL14R2	ledger inquiry		36.89	3.19	3.08	4.48	3.80	3.56	4.05	3.77
GL14R3	ledger inquiry		3	3.02	2.67	3.34	3.14	3.11	3.42	3.20
GL14R4	ledger inquiry		0.27	0.26	0.25	0.19	0.33	0.34	0.33	0.33
GL14U1	ledger inquiry		0.05	0.09	0.05	0.05	0.05	0.05	0.05	0.09
GL6R1	jour_update_display	1.06	7.16	12.72	3.8	15.36	6.77	8.13	9.39	6.31
GL6U1	jour_update_display	0.13	0.14	0.44	0.2	0.20	0.47	0.64	0.19	0.17



Data Interface Mapping System

Mainframe Custom Application

Custom Web-Based System



Identifying IT Resources (cont.)

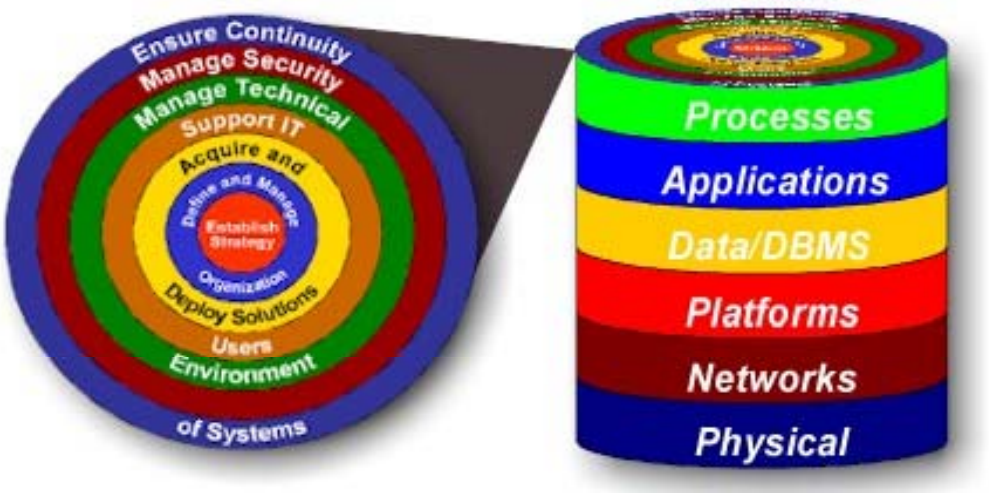
Another key step is to establish the general IT control process coverage for the identified applications.

Application Owner:	Person 1	Person 2	Person 2	Person 1	Person 1
	Application A	Application B	Application C	Application D	Application E
Change control	x		a		x
Security administration		y	z	x	
SDLC	x	b	c	x	x
Disaster recovery				x	

"Wow, we have many distinct processes which inherently introduces risk. Can we consolidate our processes to focus improvement efforts?"

Identifying IT Resources (cont.)

The application layer is the starting point for driving the assessment to deeper levels.



Planning & Strategy

- Strategy Alignment
- Organization
- Business Continuity Management

Foundation Technology Management

- Application Management
- Data/DBMS Management
- Network Management
- Platform Management

IT Operations Management

- Change Management
- Solution Development and Deployment
- Computer Operations
- Security Architecture Management
- User Support Management
- Asset Management

Service Level Management

- Service Level Management

Identifying IT Resources (cont.)

Risks need to be sourced within the applications as well.

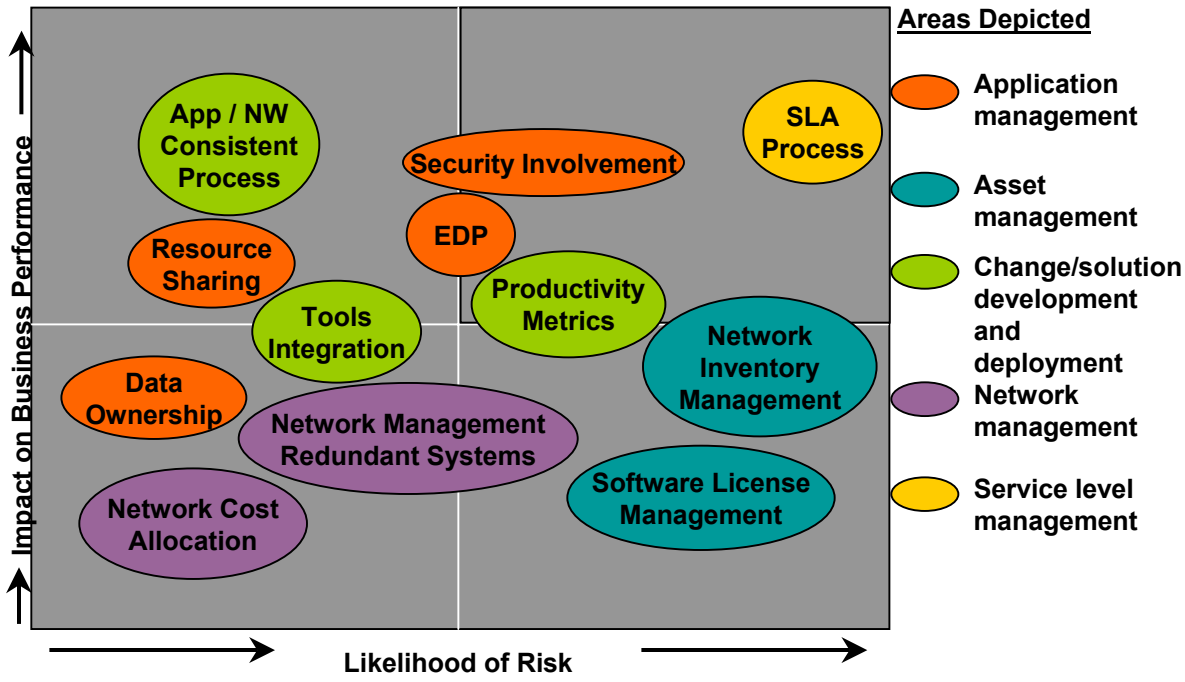
Application Owner:	Person 1	Person 2	Person 2	Person 1	Person 1
	Application A	Application B	Application C	Application D	Application E
Reports	- Report A - Report B - Report C	- Report A1 - Report B1 - Report C1	- Report A2 - Report B2 - Report C2	- Report A3 - Report B3 - Report C3	- Report A4 - Report B4 - Report C4
Check digit calculations	- Program x	- Program y - Program z		- Program a	
Edit checks		- Program f	- Program g - Program h		
Logic test validation			- Program m	- Program n	

Challenges to Identifying IT Resources

- Outsourced transaction processing
- Applications that are owned by the business
- Vendor support of packaged software
- Lack of overall documentation (Sarbanes-Oxley has helped prove this out in many public companies)
- Difficult linking IT processes to applications and to underlying technology components

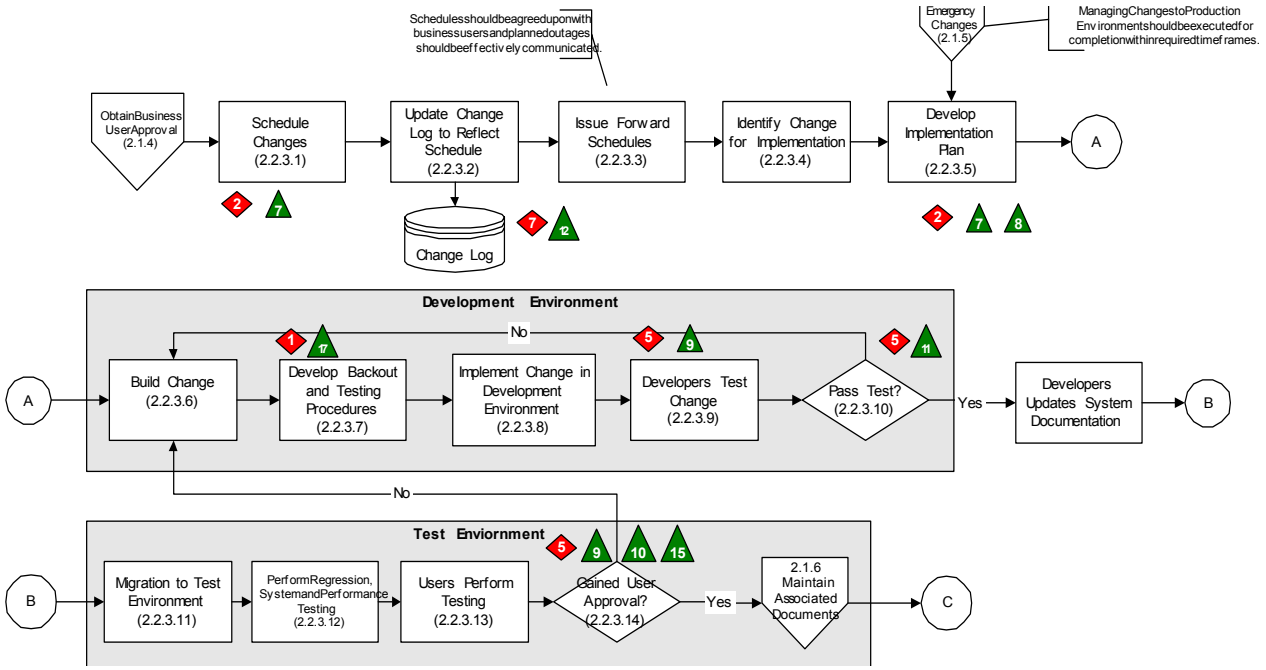
Identifying and Assessing Risks

Management will need to determine the risks associated with the control objectives and the IT resources. The established “common language” will be used to source the necessary risks.



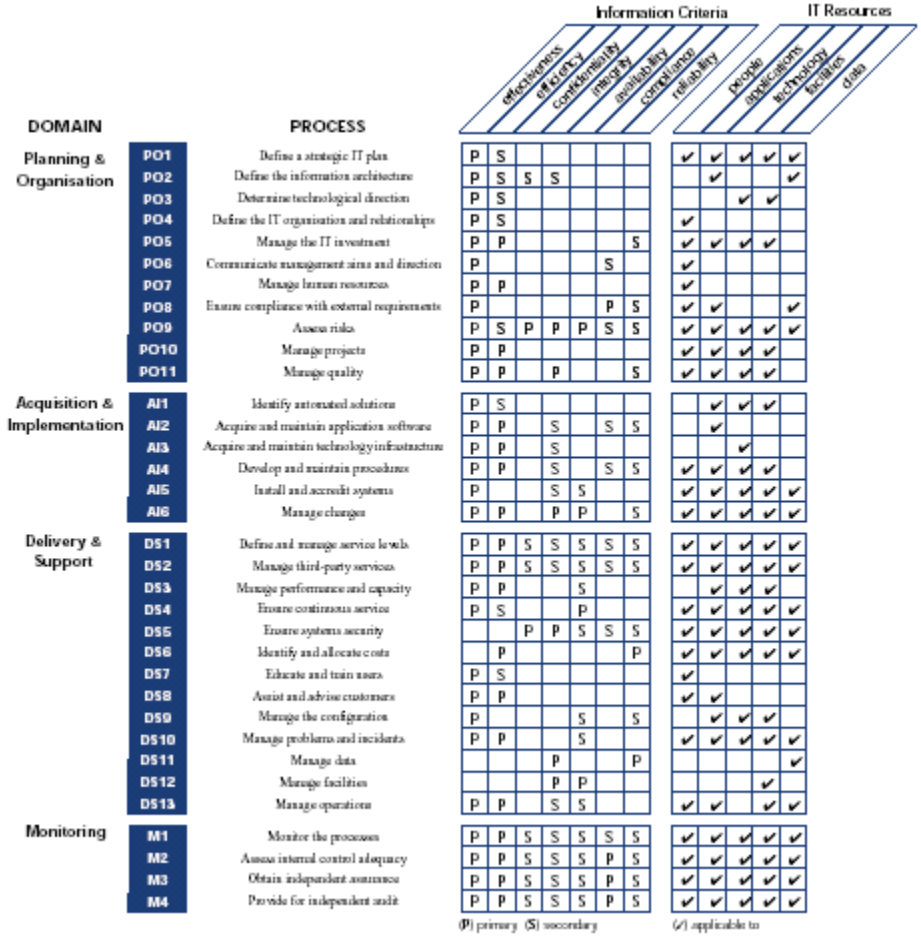
Linking Risks to Processes and Controls

The creation of detailed process flows and risk/control matrices for Sarbanes-Oxley projects has rejuvenated the skillsets associated with this key step.



Linking Risks to Processes and Controls (cont.)

The COBiT framework provides a rich repository from which to start analyzing IT's risk management coverage and applicability to the company's environment.



DOMAIN		PROCESS	Information Criteria							IT Resources				
			effectiveness	efficiency	confidentiality	integrity	availability	compliance	reliability	people	applications	technology	facilities	data
Planning & Organisation	PO1	Define a strategic IT plan	P	S						✔	✔	✔	✔	✔
	PO2	Define the information architecture	P	S	S	S					✔			✔
	PO3	Determine technological direction	P	S								✔	✔	
	PO4	Define the IT organisation and relationships	P	S						✔				
	PO5	Manage the IT investment	P	P					S	✔	✔	✔	✔	
	PO6	Communicate management aims and direction	P					S		✔				
	PO7	Manage human resources	P	P						✔				
	PO8	Ensure compliance with external requirements	P					P	S	✔	✔			✔
	PO9	Assess risks	P	S	P	P	P	S	S	✔	✔	✔	✔	✔
	PO10	Manage projects	P	P						✔	✔	✔	✔	
	PO11	Manage quality	P	P		P			S	✔	✔	✔	✔	
Acquisition & Implementation	AI1	Identify automated solutions	P	S							✔	✔	✔	
	AI2	Acquire and maintain application software	P	P		S		S	S		✔			
	AI3	Acquire and maintain technology infrastructure	P	P		S						✔		
	AI4	Develop and maintain procedures	P	P		S		S	S	✔	✔	✔	✔	
	AI5	Install and accredit systems	P			S	S			✔	✔	✔	✔	✔
	AI6	Manage changes	P	P		P	P		S	✔	✔	✔	✔	✔
Delivery & Support	DS1	Define and manage service levels	P	P	S	S	S	S	S	✔	✔	✔	✔	✔
	DS2	Manage third-party services	P	P	S	S	S	S	S	✔	✔	✔	✔	✔
	DS3	Manage performance and capacity	P	P			S				✔	✔	✔	
	DS4	Ensure continuous service	P	S			P			✔	✔	✔	✔	✔
	DS5	Ensure systems security			P	P	S	S	S	✔	✔	✔	✔	✔
	DS6	Identify and allocate costs		P					P	✔	✔	✔	✔	✔
	DS7	Educate and train users	P	S						✔				
	DS8	Assist and advise customers	P	P						✔	✔			
	DS9	Manage the configuration	P				S		S		✔	✔	✔	
	DS10	Manage problems and incidents	P	P			S			✔	✔	✔	✔	✔
	DS11	Manage data				P			P					✔
	DS12	Manage facilities				P	P						✔	
	DS13	Manage operations	P	P		S	S			✔	✔		✔	✔
Monitoring	M1	Monitor the processes	P	P	S	S	S	S	S	✔	✔	✔	✔	✔
	M2	Assess internal control adequacy	P	P	S	S	S	P	S	✔	✔	✔	✔	✔
	M3	Obtain independent assurance	P	P	S	S	S	P	S	✔	✔	✔	✔	✔
	M4	Provide for independent audit	P	P	S	S	S	P	S	✔	✔	✔	✔	✔

(P) primary (S) secondary (✔) applicable to

Measuring the Technology Risks

Capability Maturity Continuum provides a framework for improving processes

Capability Level	Capability Description
Optimizing	**CONTINUOUS IMPROVEMENT** Continuously improving controls enterprise-wide
Managed	**QUANTITATIVE** Risks managed quantitatively enterprise-wide "Chain of accountability"
Defined	**QUALITATIVE/QUANTITATIVE** Policies, process and standards defined and institutionalized -- "Chain of certification"
Repeatable	**INTUITIVE** Process established and repeating; reliance on people continues -- Controls documentation lacking
Initial	**AD HOC/CHAOTIC** Control is not a priority -- Unstable environment leads to dependency on heroics

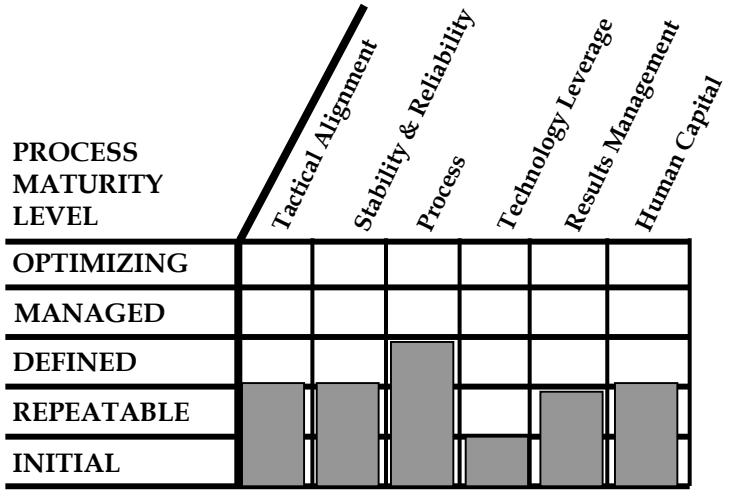
Derived from Carnegie Mellon capability maturity model

Process maturity – How is it defined?

Assess Process Maturity with six (6) distinct attributes:

- Tactical Alignment
- Stability & Reliability
- Process
- Technology Leverage
- Results Management
- Human Capital

Maturity



evaluation…

Work includes:

- Interviews
- Documentation reviews
- Observation of management processes

Risks

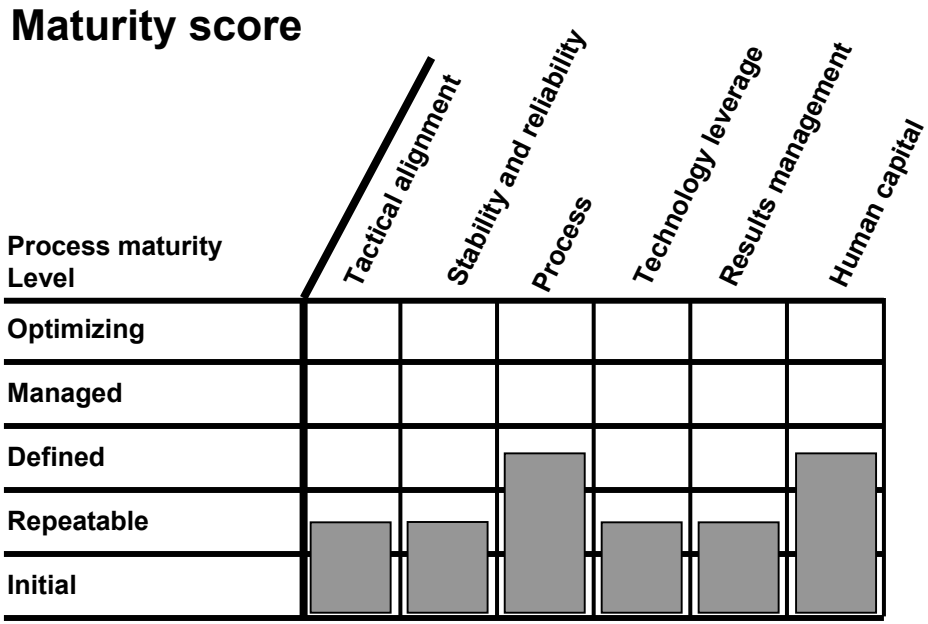
Evaluation Criteria	Strengths	Improvement Opportunities/Risks
Tactical Alignment The strategy and organizational struct the IT department is properly aligned wit business to ensure IT activities are in direct support of critical business processes.	The IT organization is meeting the primary needs	None
Stability and Reliat The technology architecture and hun resource components appropriate to carry the mission of the department.		

Evaluation Criteria	Strengths	Improvement Opportunities/Risks
Process IT functions performed are managed as business processes.	IT management has implemented several formal processes to improve the overall quality of service delivered to	See each IT infrastructure area for area specific process improvements.
Technology Leverage IT management utilizes technology effectively to automate management processes, where appropriate.		
Results Management IT processes are measured for effectiveness and the measurements (metrics) are reported to the company.		

Evaluation Criteria	Strengths	Improvement Opportunities/Risks
Results Management (cont.)	IT is also responsible for meeting specific service level agreements with strategic business partners related to provisioning and page out unctions.	There is a risk that the company is setting goals that either are not meeting the needs of the business, or, possibly in the future, exceeding the needs of the company which may potentially lead to overspending on the IT function. This risk is compounded by the fact the user community is not interested in understanding how specific IT performance affects their ability to meet their key success factors.
Human Capital "People processes" are given the appropriate level of attention to help ensure the department maintains its intellectual capital.	There are strong "people processes" in place within the IT department. Over the past 18 month, IT management has rationalized the number of positions/levels within IT. This was followed by clear and communicated career progression possibilities within the IT department. To support career progression (and to ensure WebLink is maintaining quality IT personnel) a formal goal setting and review process has been established and is consistently followed throughout IT. This process includes an automation to enforce the review process and maintain metrics on individual performance on an annual basis. In addition to rationalizing the number of positions/levels within IT, senior IT management has also acquired necessary director/manager skills to support the implementation of the IT strategic plan The use of contractors/consultants is limited to either supplement technical skill deficiencies or to address "one-time" projects. There is not a tremendous reliance on consultants or contractors for day-to-day operations or for "mission critical" initiatives of the business, allowing the company to maintain knowledge capital in-house.	Although the IT department has accomplished significant improvements related to human resource management, the attrition rate within IT is still fairly high (25%-30%). The majority of people who have left site compensation as their number one motivator for accepting new positions. IT management does not have the ability in selective situations, to make counter-offers to valuable employee's the company wishes to retain. It is understood that compensation studies have been performed. However, WebLink positions were benchmarked against other wireless (paging) communication companies in the Metroplex and not against other high technology companies for which IT is competing to obtain/retain human resources.. There is a risk the attrition rate within IT will continue at its current pace, or increase, if the compensation issues are not formally addressed.

Example Assessment

APPLICATION AND DATA MANAGEMENT



Technology management recommendations

1. Implement productivity and quality measures in application management
2. Involve corporate security in the development and design of the network systems applications
3. Increase resource-sharing efficiencies between development groups
4. Integrate all relevant players into the SDLC implementation
5. Implement data ownership by business process owners

Example Assessment (cont.)

APPLICATION AND DATA MANAGEMENT

Involve corporate security in the development and design of the systems applications
Priority: High
Risk addressed: Stability and reliability

IT organizations must provide services in a manner that is not only responsive, reliable and cost-efficient, but also secure. The goal of application management is to leverage the power and potential of deployed applications while guaranteeing the availability, performance, capacity and integrity of applications to meet prescribed service levels. If Corporate Security is not involved in the development and design of network systems applications there may continually be unscheduled downtime resulting in business process interruptions.

Implement productivity and quality measures in application management
Implementation priority: High
Risk addressed: Results management

SDLC group needs to establish valid application development metrics (besides LoE) so that it can track successes and establish sound strategies for improved performance. Enhanced metrics provide a qualitative as well as a quantitative measure of how processes/resources are performing and what can be done to improve performance in terms of efficiency and effectiveness. Some metrics that that should be captured include:

- Percent of user or client requirements that can be met by existing systems versus those requiring new solutions.
- Average elapsed turnaround time to deliver strategic solutions to market.
- Percent of new projects meeting original functional requirements.
- Project cost as a percentage of savings realized.
- Cost of application maintenance attributed to quality issues.
- Number of problems by application. Trends over time.

Value Proposition

Meeting the Challenge of Skeptics

SKEPTIC	VALUE PROPOSITION	VALUE TYPE
CIO	Better business alignment	
	Process maturity	$ 
	Comprehensive IT asset inventory	$
	Robust IT risk inventory	$ 
	Improved delivery results (infrastructure, application development efforts, vendor management, etc.)	$ 

Meeting the Challenge of Skeptics (cont.)

SKEPTIC	VALUE PROPOSITION	VALUE TYPE
CFO	Greater awareness of technology impact	 $ 
	More informed risk assessment process	 $
	Operating effectiveness opportunities/better usage of technology capital investments	$

Meeting the Challenge of Skeptics (cont.)

SKEPTIC	VALUE PROPOSITION	VALUE TYPE
Business Department Lead	Greater awareness of technology impact	 $ 
	More informed risk assessment process	 $
	Increased coordination / collaboration with IT	
	Better utilization of IT assets for competitive advantage	$ 

Getting Off the Starting Line

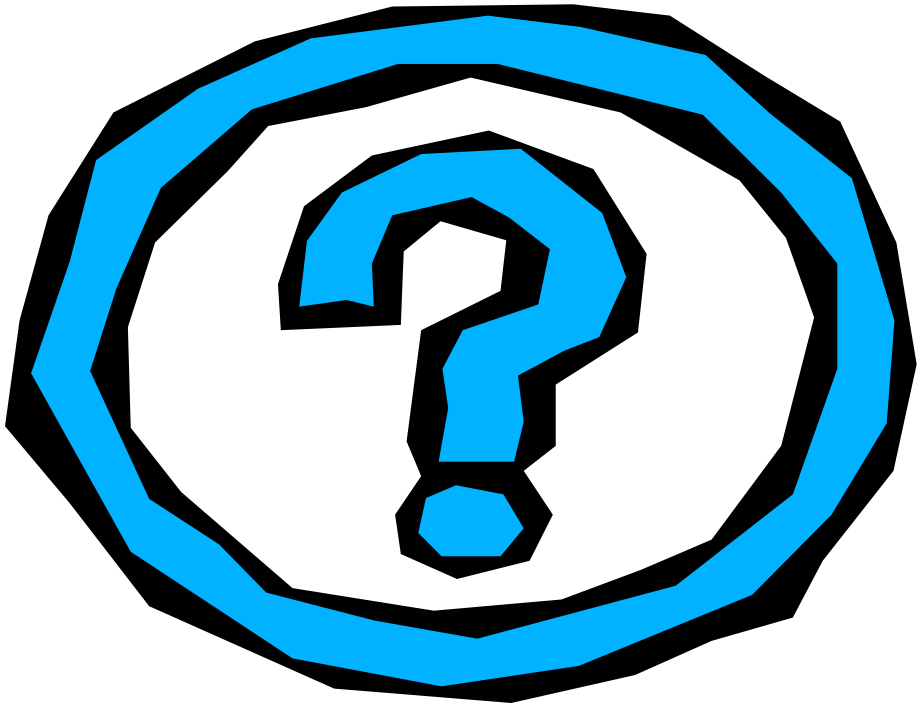
How do I go from here?

- Leverage results from other compliance efforts (documentation, self-assessment processes, ERM structure, etc.)
- Develop your application inventory and confirm ownership
- Develop your general IT control coverage for these applications
- Communicate process improvement opportunities for distinct general IT processes
- Select one IT process management scope area (database management, network management, IT operations management, etc) or application
- Select one business department to pilot developing the risk profile for the IT process management/application scope area
- Ensure IT representation/participation with ERM oversight and planning activities

How do I go from here? (cont)

- Establish realistic maturity goals but measure them rigorously
- “Wow” the skeptics by illustrating the resulting value
- Leverage other company initiatives, such as ISO9001 or ISO/IEC 17799, as you proceed down the path or ERM

Questions



Tom Andreesen

913-685-6241

Thomas.Andreesen@protiviti.com