The San Francisco Chapter of ISACA proudly presents...
SF ISACA 2007 Fall Conference
IT Audit
Information Security
IT Governance
Risk Management
Compliance

IT Risk Assessment

Jerry Meyers, Protiviti

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Learning Objectives

- ✓ Define risk
- ✓ Define risk assessment
- ✓ Understand how an IT Risk Assessment fits into an organization's overall Risk Assessment activities
- ✓ Describe an IT Risk Assessment Approach
- ✓ Describe how risks are identified and prioritized
- ✓ Define Risk Oversight Responsibility
- ✓ Distinguish between Assessments for Internal Audit vs. the CIO

Setting the Foundation

What is Risk?

COSO Definition:

The possibility that an event will occur and adversely affect the achievement of objectives

What is Risk Assessment?

Risk assessment is the identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed.

COSO Internal Control Integrated Framework

What Protiviti’s specialists say about risk assessment?

“The process applied through quantities and qualitative means to consider both:

(a) The likelihood of potential events occurring over a clearly defined time horizon and

(b) The impact of those potential events, if they were to occur on the achievement of key business objectives.

Risks may be assessed on both an inherent and a residual basis.

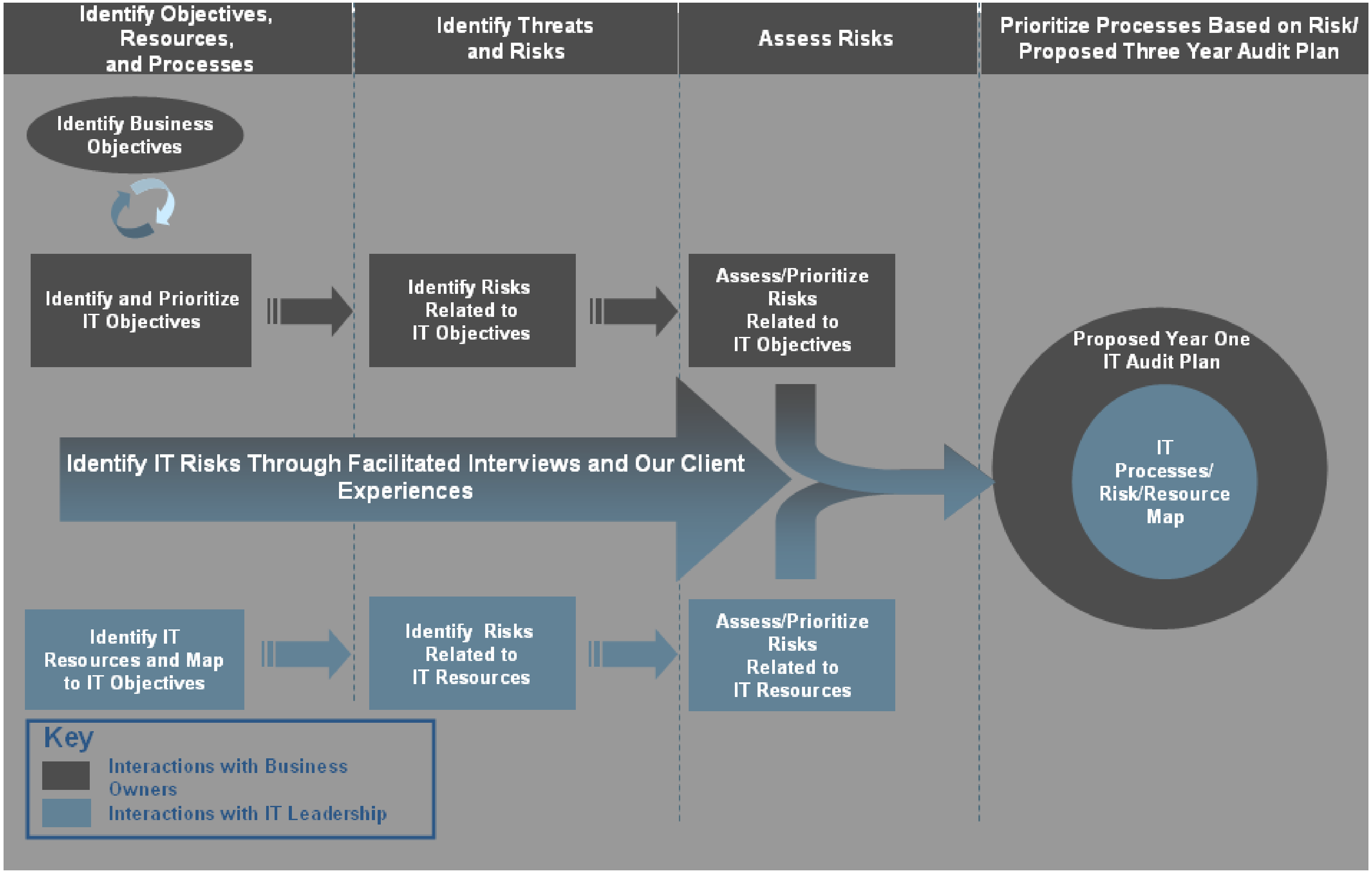
Jim DeLoach

Protiviti Managing Director

IT Risk Assessment

Overview

IT Risk Assessment Approach

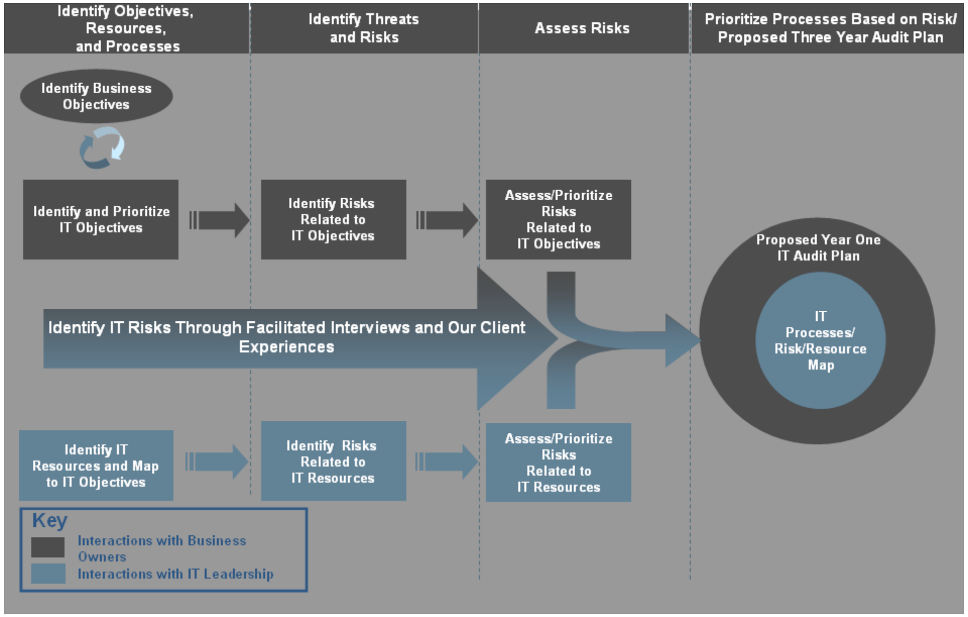

Identify Objectives, Resources, and Processes
Identify Threats and Risks
Assess Risks
Prioritize Processes Based on Risk/ Proposed Three Year Audit Plan
Identify Business Objectives
Identify and Prioritize IT Objectives
Identify Risks Related to IT Objectives
Assess/Prioritize Risks Related to IT Objectives
Proposed Year One IT Audit Plan
IT Processes/ Risk/Resource Map
Identify IT Risks Through Facilitated Interviews and Our Client Experiences
Identify IT Resources and Map to IT Objectives
Identify Risks Related to IT Resources
Assess/Prioritize Risks Related to IT Resources
Key
Interactions with Business Owners
Interactions with IT Leadership

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

IT Risk Assessment Approach

Drivers:

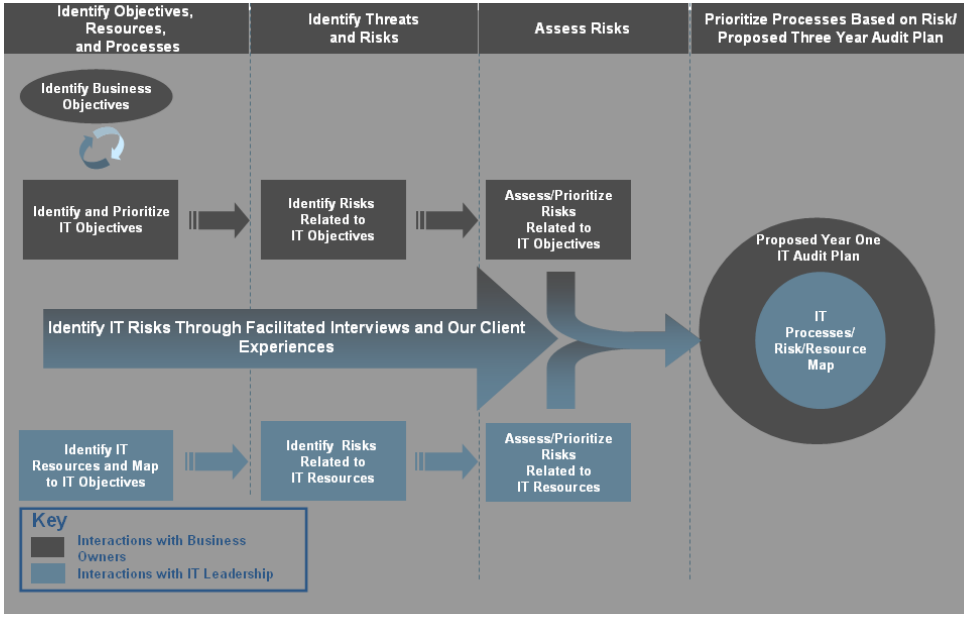
- ✓ Scope
- ✓ Resources
- ✓ Objective / Audience


Identify Objectives, Resources, and Processes
Identify Threats and Risks
Assess Risks
Prioritize Processes Based on Risk/ Proposed Three Year Audit Plan
Identify Business Objectives
Identify and Prioritize IT Objectives
Identify Risks Related to IT Objectives
Assess/Prioritize Risks Related to IT Objectives
Identify IT Risks Through Facilitated Interviews and Our Client Experiences
Proposed Year One IT Audit Plan
IT Processes/ Risk/Resource Map
Identify IT Resources and Map to IT Objectives
Identify Risks Related to IT Resources
Assess/Prioritize Risks Related to IT Resources
Key
Interactions with Business Owners
Interactions with IT Leadership

IT Risk Assessment Approach

Approach:

- ✓ Interviews
- ✓ Surveys
- ✓ Use of Tools



Identify Objectives, Resources, and Processes

Identify Threats and Risks

Assess Risks

Prioritize Processes Based on Risk/ Proposed Three Year Audit Plan

Identify Business Objectives

Identify and Prioritize IT Objectives

Identify Risks Related to IT Objectives

Assess/Prioritize Risks Related to IT Objectives

Identify IT Risks Through Facilitated Interviews and Our Client Experiences

Proposed Year One IT Audit Plan

IT Processes/ Risk/Resource Map

Identify IT Resources and Map to IT Objectives

Identify Risks Related to IT Resources

Assess/Prioritize Risks Related to IT Resources

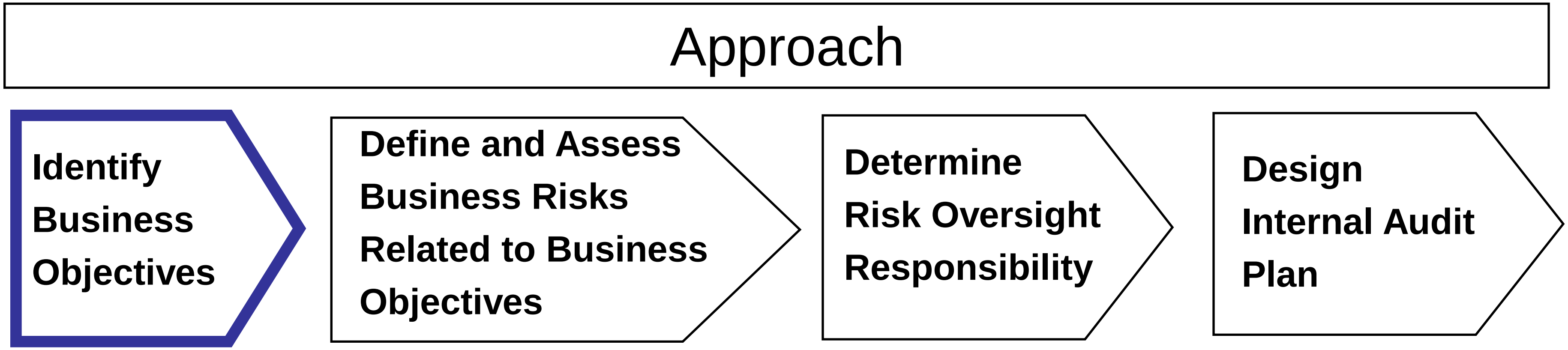
Key

■ Interactions with Business Owners

▨ Interactions with IT Leadership

Step 1 – Identify Business Objectives

Identify and Assess Risk at Entity Level



Approach

Identify Business Objectives

Define and Assess Business Risks Related to Business Objectives

Determine Risk Oversight Responsibility

Design Internal Audit Plan

Objectives

- Identify, define and understand operational, compliance and financial reporting objectives

Key Tools

- Risk Models (industry, etc)
- Internal and external sources of information

Identifying Business Objectives

- ✓ Objective setting is a key part of the management process
- ✓ Objectives are prerequisites to and enablers of internal control
- ✓ Objectives may be explicitly stated, or be implicit
- ✓ Sub-Objectives, or activity-level objectives, should be included

Understanding the Business

Environment

Widget manufacturers are aggressively pursuing strategies to reduce their overall cost-of-test by increasing the throughput of their test systems. Cost-of-test includes the initial ATE and ancillary equipment purchase price, as well as set up and operating cost, and is often the most significant manufacturing cost, particularly for high volume, low cost devices. For these types of devices, ATE throughput, or the number of devices that can be tested in a given unit of time on a single test system, is a key determinant of cost-of-test per device and of a manufacturer's ability to compete profitable.

Value

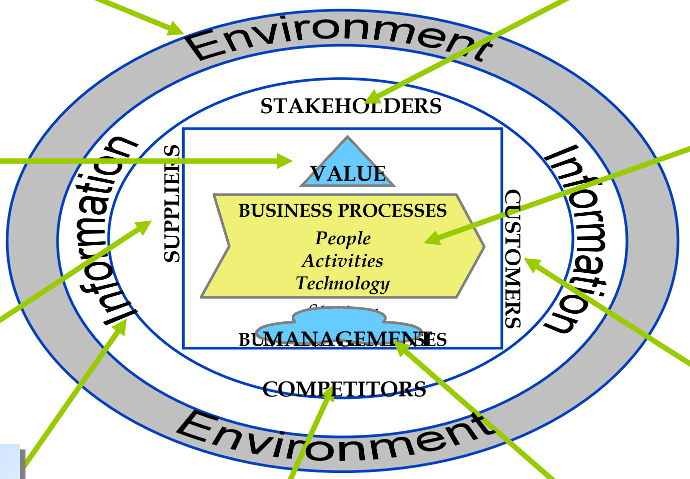
- Company X market understanding, coupled with the breadth and depth of their design-to-production test product portfolio, makes them an ideal choice for integrated device manufacturers, fabless semiconductor companies, outsource assembly and test suppliers and foundries.
- Company X leads the industry in addressing new wireless challenges with patented technologies such as modulated vector network analysis (MVNA).
- Company X is one of the very few test system manufacturers that provides its customers with flexible and creative financial structures.
- The Company X Super D-10 system has been honored with a 2003 Test & Measurement World Best in Test award.
- In 2004, Company X received Top ATE Supplier Ranking in VLSI Research Customer Satisfaction for Third consecutive year.

Suppliers

Company X relies on outside vendors to manufacture certain components and subassemblies. Company X seeks to manage their inventory levels through agreements with both suppliers and subcontractors that provide just-in-time delivery of these components and subassemblies

Information

Fiscal 2006 Revenue $874.4 Million USD
Net Income Fiscal Year Ended Oct 31st 2006 (Loss) $181,585 (in thousands)
Employees 1738 direct employees and 25 temporary employees
Headquarters San Jose, California
Locations Over 35 location in 20 countries worldwide.
Major Location(s) California, Iowa, Texas, Montana, UK, Asia
Major Systems SAP (US) and Various (everywhere else)
Established Founded in 1976 and incorporated in 1984 San Jose, California
Publicly Held New York Stock Exchange ABCD
Subsidiaries Company X Systems Benelux (Belgium), Beijing office and Shanghai office (China), France, Company X Systems GmbH Amerang and Company X Systems GmbH (Germany), DVS India (P) Ltd (India), ABCD Engineers Ltd (Israel), Company X Systems Italy (Italy), Company X Systems K.K (Japan), Company X Korea (Korea), Company X Systems (M) Sdn Bhd (Malaysia), Company X Systems (P), Inc and UST Technology (Philippines), Company X Systems Pte Ltd (Singapore), Asia Repair Center (Taiwan), and Company X (UK).



Competitors

Advantest Corporation – Santa Clara, California
Eagle Test Systems, Inc. – Chicago, Illinois
DEF Corporation – Norwood, Massachusetts
Nextest Systems Corporation – San Jose, California
Teradyne Inc. – North Reading, Massachusetts
Verigy Ltd – Cupertino, California
ABC Company – Hillsboro, Oregon
Hamamatsu Corporation – Hamamatsu City, Japan

Owners

Company X is a publicly traded company. Market Cap as of Jan 18th 2007 stands at 900.90 M.

	Preferred Stock	**Common Stock**
Shares Outstanding	0	200,610
Shares Issued	0	200,610
Shares Authorized	71,304	250,000

Business Processes

- Company X is a leading provider of test and diagnostic solutions for the consumer age integrated circuit industry. They design, manufacture, sell and service engineering validation test equipment, diagnostic and failure analysis products and automatic test equipment, or ATE, used for testing semiconductor integrated circuits, or ICs. Company X delivers competitive cost and performance advantages to integrated device manufacturers (IDMs), wafer foundries, outsourced assemble and test (OSAT) suppliers and fabless chip companies worldwide.

Customers

Company X top 3 customers	**% of Revenue in 2006**
AMD	23%
Intel	15%
Spirox	13%

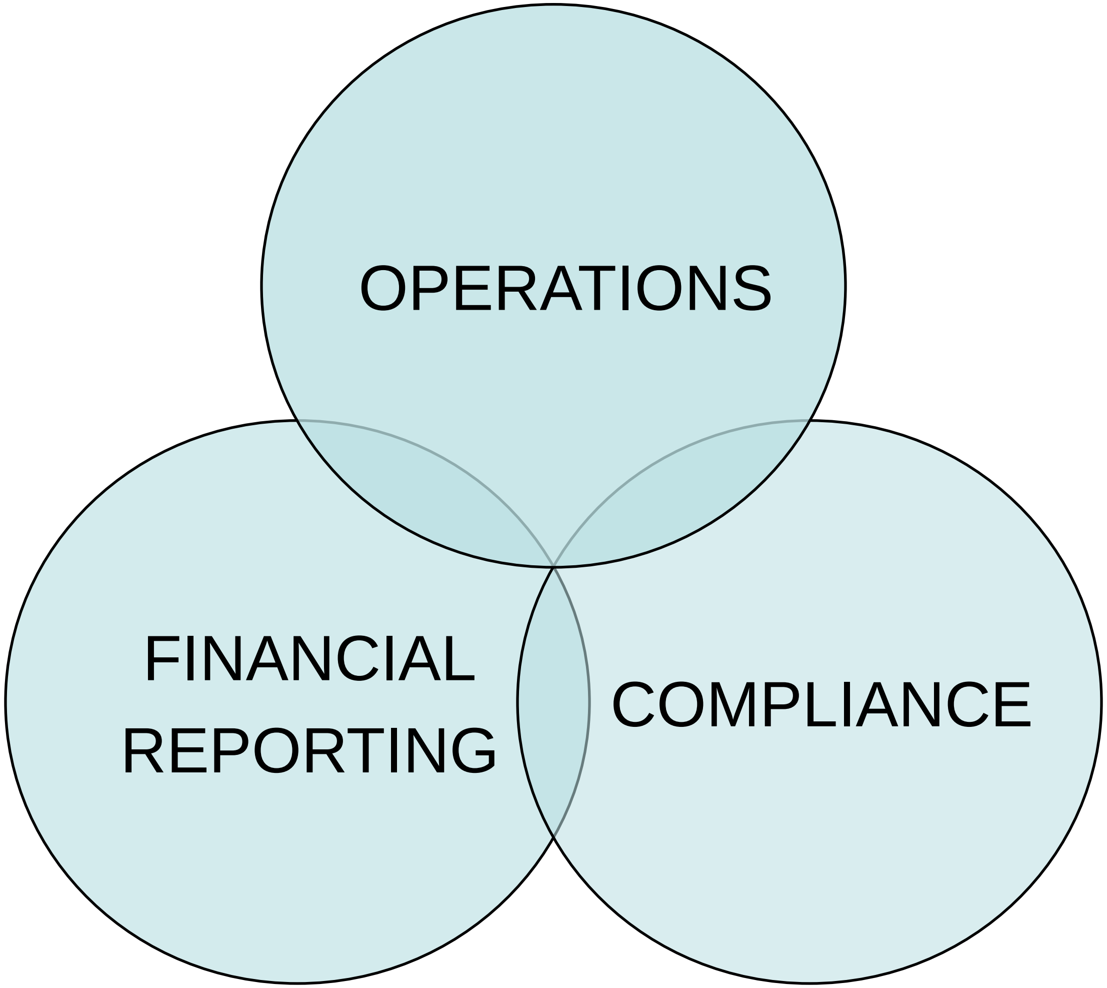
- Company X customer's design, manufacture and test semiconductors in high volume for use in applications such as automobile, appliances, personal computers, mobile consumer electronic, digital television, wireless LAN and multimedia hardware.

Management

Executive officers:
Barry White – Chairman
Tina Turner – President and CEO
Ottis Redding – CFO
John Smith – Sr. Vice President and general counsel
Jose Montana – Sr. Vice President, Products
Jerry Rice – Sr. Vice president, World Wide Field operations
Tiger Woods – Sr. Vice President, Manufacturing Operations

Key Employees:
Joseph Schmo – Vice President, Strategy and Business Development
Randy Moss – Vice President, Chief Information Officer
George Bush – Vice President, Human Resources

Business Objectives



Operations Objectives

Operations Objectives relate to achievement of an entity's basic mission. For Example:

Objective	Example
Growth	Grow Revenue by 20%
Geography	Enter Japanese Market
Infrastructure	Install New ERP application
Profitability	Earnings per share (EPS) of $1.25
Product	Develop second generation of product X
Customer Quality	Rating 4.5 out of 5

Compliance Objectives

An entity must conduct it’s activities, and often take specific actions, in accordance with applicable laws and regulations, such as:

- Securities and Exchange Commission (SEC) reporting
- Generally Accepted Accounting Principles (GAAP)
- Gramm-Leach-Bliley Act (GLBA)
- Sarbanes-Oxley
- Occupational Safety and Health Administration (OSHA)
- Food and Drug Administration (FDA)
- Federal Deposit Insurance Incorporation Improvement Act (FDICIA)
- Public Utilities Commission (PUC)
- Tax status
- Human resources regulations (e.g. I-9)

Financial Objectives

Since the advent of SOX, financial objectives have been most of the focus from:

Objective	Example
Accuracy	Capture every transaction at the correct amount
Timeliness	Capture every transaction in the proper period
Completeness	Capture all necessary transactions that occurred
Valid	Each transaction represents an actual event
Efficiency	Close books within 8 business days

Key Ideas

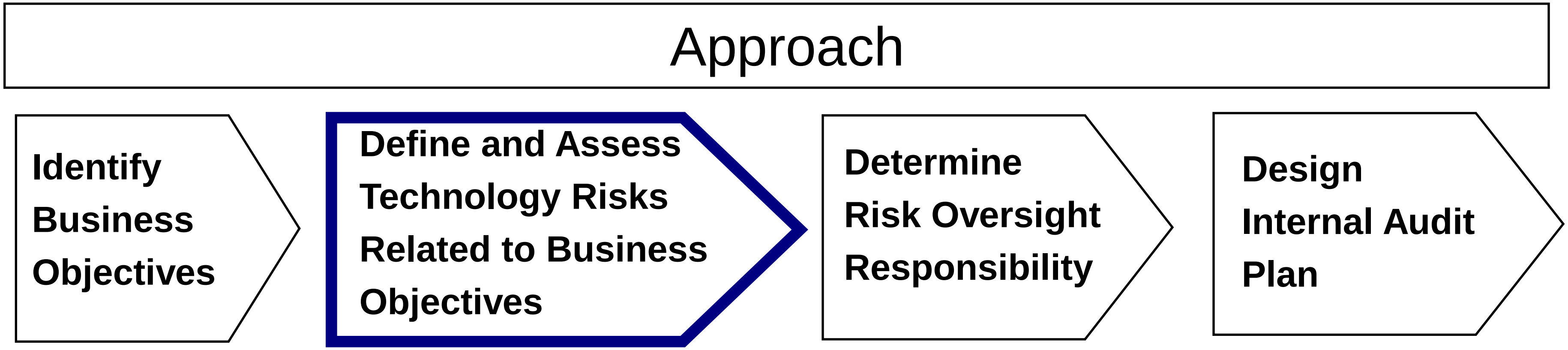
- Objectives must first be identified before risks to their achievement can be identified
- Risk is the possibility that an event will occur and adversely affect the achievement of objectives
- Risk assessment is the identification and analysis of relevant risks to achievement of objectives, forming a basis for determining how the risks should be managed

Key Ideas (cont.)

- The overall business must be understood in order for objectives and risks to have the proper context
- The IT Risk Assessment process must be tailored based on the final objective and the level of effort that can be dedicated

Step 2 – Define and Assess Technology Risks

Identify and Assess Risk at Entity Level



Approach

Identify Business Objectives

Define and Assess Technology Risks Related to Business Objectives

Determine Risk Oversight Responsibility

Design Internal Audit Plan

Objectives

- Identify, define and understand technology risks as they relate to the areas of the business they support

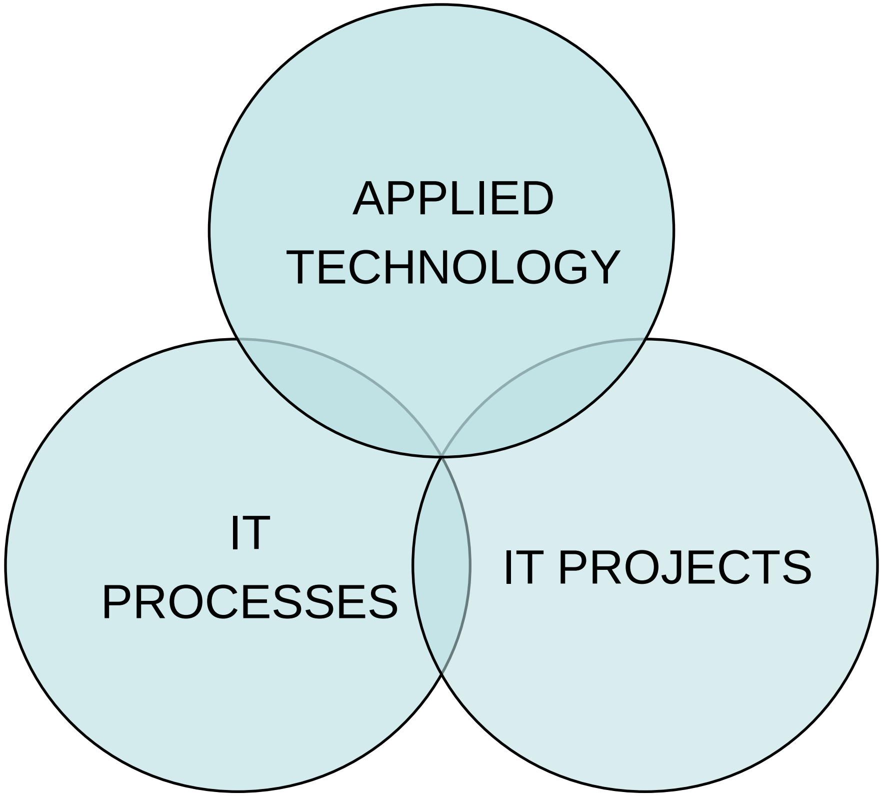
Key Tools

- Risk Models (industry, etc)
- Internal and external sources of information

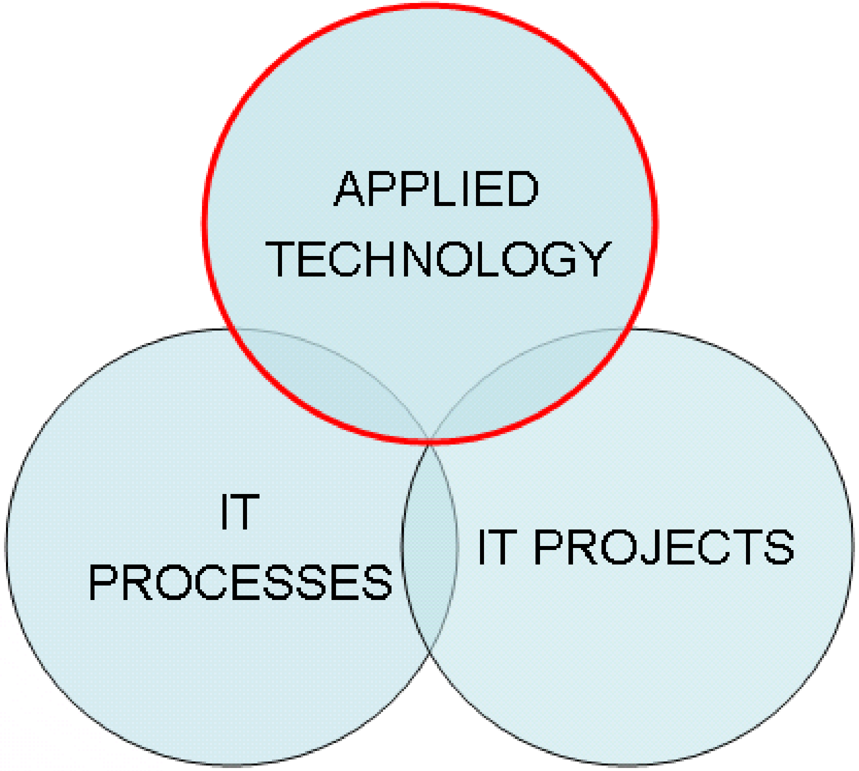
IT Risk Assessment Approach

The 3 Areas of IT Risk Impact.

- Applied Technology
- IT Processes
- IT Projects

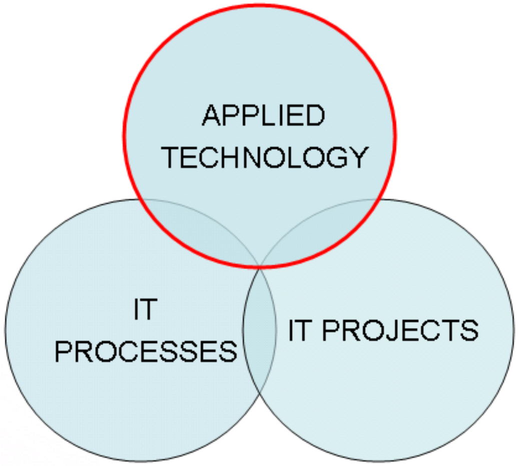


Applied Technology



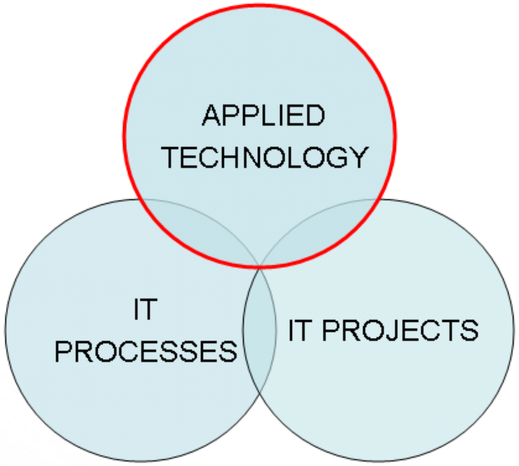
Applied Technology

- Applications
- Key Devices
- Utilities
- The Context
  - – Business Cycles
  - – Business Entities
  - – Business Partners



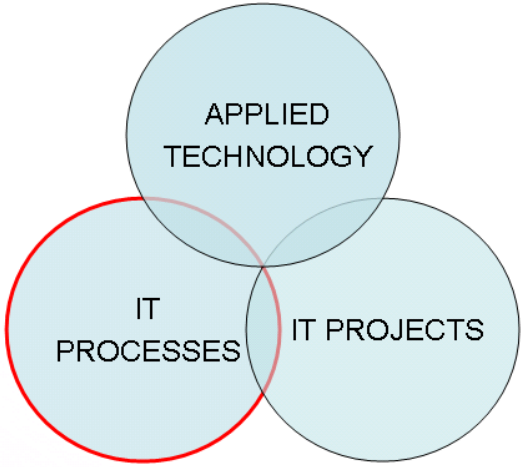
Risk Ranking – Applied Technology

- Criteria Evaluated:
  - Stability
  - Integrity
  - Sensitivity
  - Complexity
  - Financial Exposure



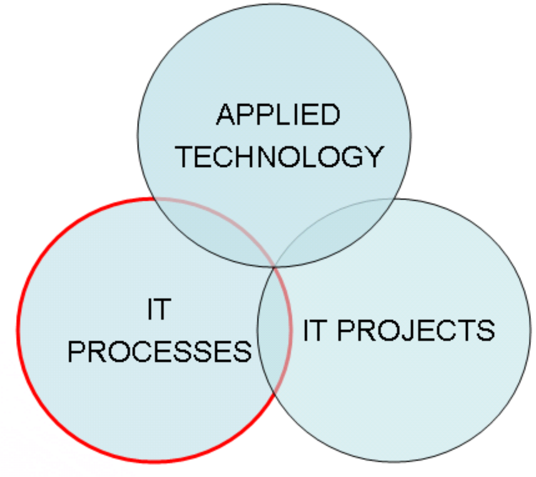
IT Processes

- Framework
  - CobiT
  - ITIL
  - ITPI
- The Context
  - Organizational Structure
  - “Rogue” IT Groups
  - Business Partners



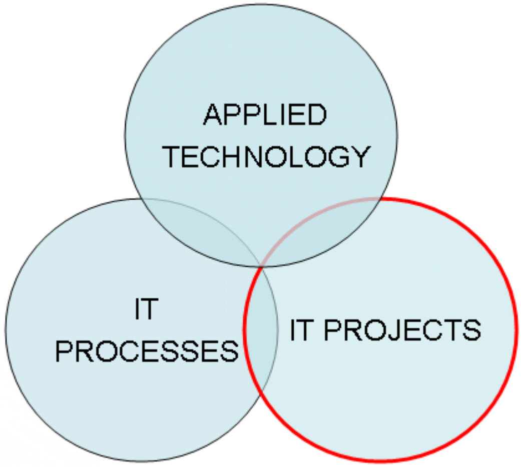
Risk Ranking – IT Processes

- Criteria Evaluated:
  - Reliability and Efficiency
  - Consistency
  - Technology Leverage
  - Results Management
  - Human Capital
  - Complexity



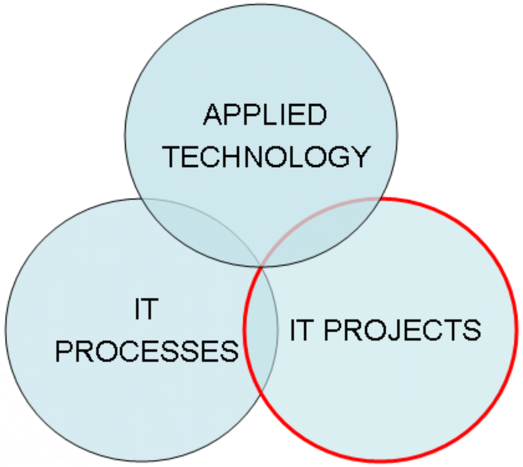
IT Projects

- Considerations
  - Timing
  - Area(s) Impacted
  - Ownership
  - PMO?



Risk Ranking – IT Projects

- Criteria Evaluated:
  - Criticality
  - Project Management Experience
  - Executive Ownership
  - Process and Control Reengineering
  - Development Platform
  - Custom Programming
  - Project Budget



Putting It All Together

Identifying Risk

- **Not all risks in a given Risk Model must be addressed by every organization**

- **Management should determine how they will quantify:**
  - Their risk appetite
  - The likelihood a risk may occur
  - The potential impact to the business should a risk occur

- **Evaluate each risk in the Risk Universe**

- **The cumulative results of this evaluation are used to prioritize the attention to and method of responding to each risk**

Risk Inventory

- Catalogue results
- Source as inherent or residual

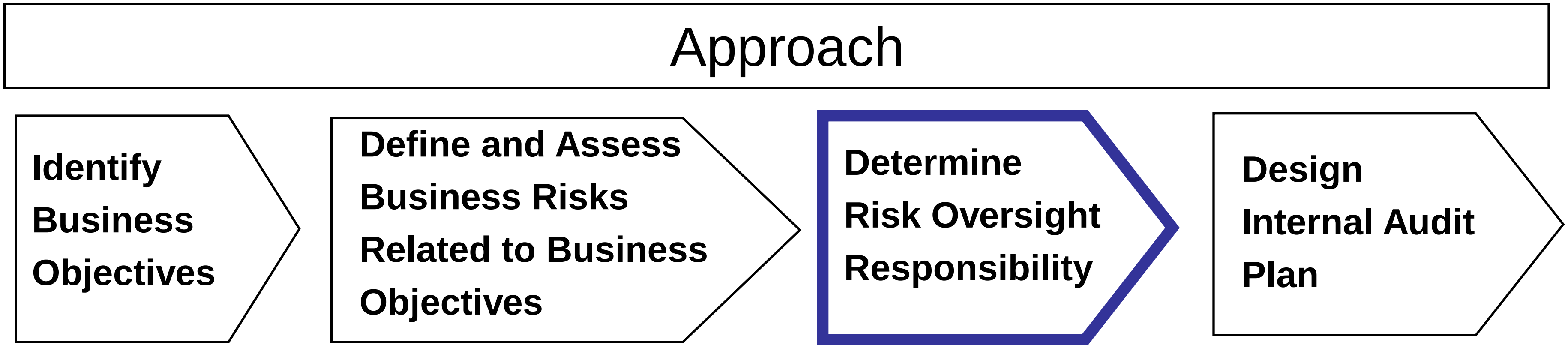
	Risk Area	Description of Risk	Who?	Residual Risk	
				Impact	Likelihood
1	Project: Outsource Manufacturing to Asia	IT may not be prepared to support new business initiatives --- IT operations do not exist in Asia	CFO, CIO	H	Inherent - H
2	Applications - SAP	SAP as currently implemented does not sufficiently support the following business needs: --- Order Management, bookings, consolidation --- Product and cost hierarchies for computation of COGS --- Workflow - purchase reqs, travel expenses, sign-offs	CFO, CIO	H	Residual - H
3	Intellectual Property – Data Privacy	Poor structure around data privacy coupled with incidents in the following areas: --- SSN Project underway but no structure exists around data privacy / data classification / data protection --- Increased risk in Asia outsourcing and 3rd party partners --- Japanese and European Data Privacy laws	CFO, Ctlr Legal	H	Both - M

Responding to Risk

- Acceptance
  - The organization chooses to accept that a risk may occur. No additional changes to business processes are made.
- Avoidance
  - The organization changes their business plans to eliminate the risk.
- Transference
  - The organization shifts the risk to another party.
- Mitigation
  - The organization takes some action to lessen the likelihood and impact should a risk occur.

Step 3 – Determine Risk Oversight Responsibility

Determine Risk Oversight Responsibility



Approach

Identify Business Objectives

Define and Assess Business Risks Related to Business Objectives

Determine Risk Oversight Responsibility

Design Internal Audit Plan

Objectives

- Determine who will be responsible for responding to each key business risk

Key Tools

- Risk Oversight Responsibility Document

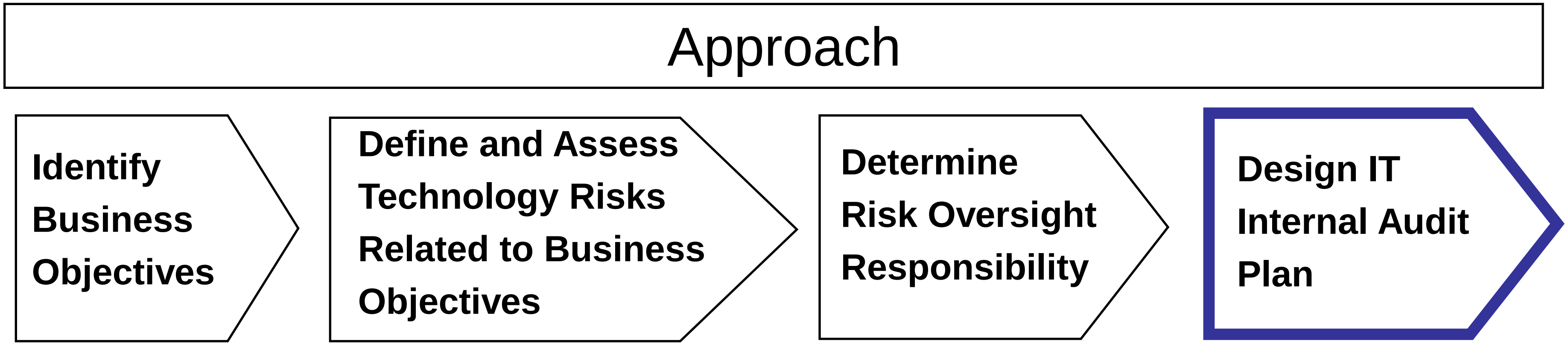
Document Risk Oversight Responsibility

- Identifies who will have oversight responsibility for each risk
- Allows IA to determine risk coverage

	Risk Area	Description of Risk	Who?	Residual Risk		Oversight Resp
				Impact	Likelihood	
1	Project: Outsource Manufacturing to Asia	IT may not be prepared to support new business initiatives --- IT operations do not exist in Asia	CFO, CIO	H	Inherent - H	Mgt / IA
2	Applications - SAP	SAP as currently implemented does not sufficiently support the following business needs: --- Order Management, bookings, consolidation --- Product and cost hierarchies for computation of COGS --- Workflow - purchase reqs, travel expenses, sign-offs	CFO, CIO	H	Residual - H	Mgt / IA
3	Intellectual Property – Data Privacy	Poor structure around data privacy coupled with incidents --- SSN Project underway but no structure exists around data privacy / data classification / data protection --- Increased risk in Asia outsourced and 3rd party partners --- Japanese and European Data Privacy laws	CFO, Ctlr Legal	H	Both - M	IA / Legal

Step 4 – Design IT Internal Audit Plan

Design IT Internal Audit Plan



Approach

Identify Business Objectives

Define and Assess Technology Risks Related to Business Objectives

Determine Risk Oversight Responsibility

Design IT Internal Audit Plan

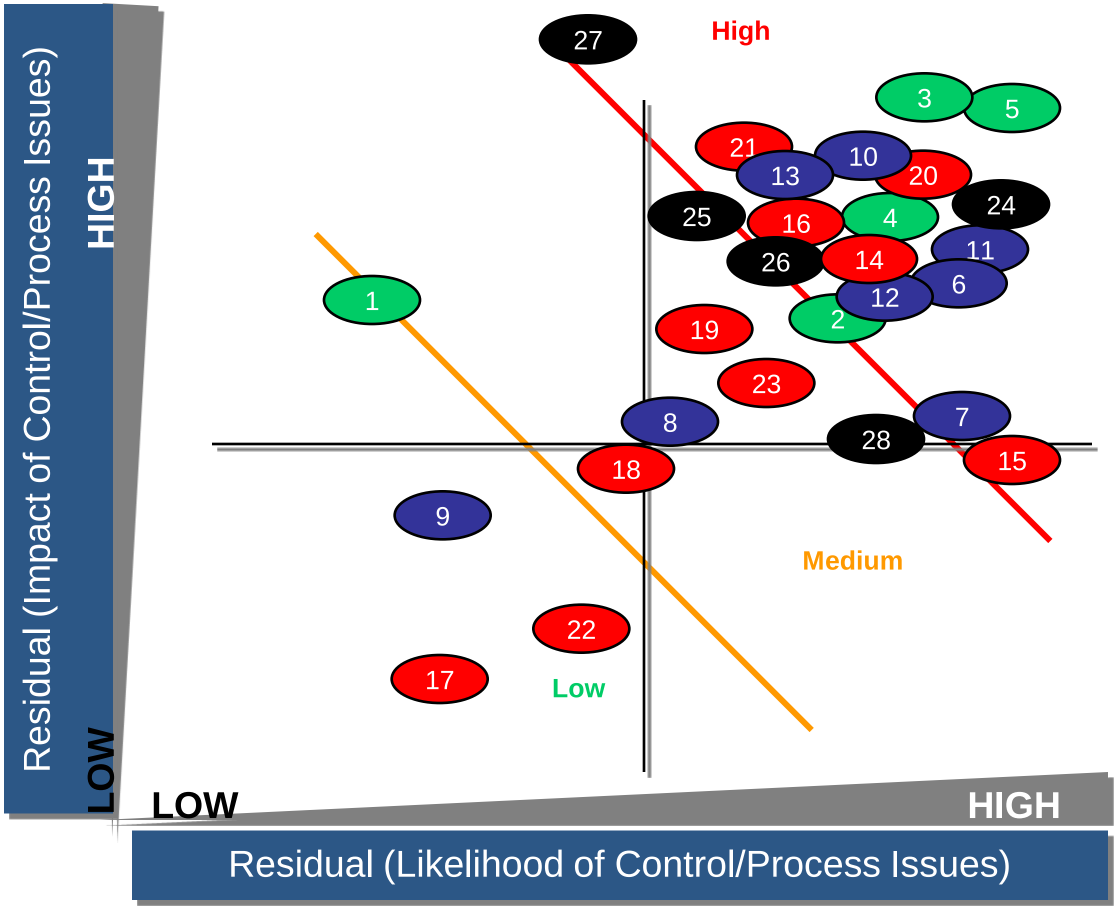
Objectives

- Translate Identified Risks Into Project Coverage

Key Tools

- Risk Map
- Audit Plan

Evaluate Risk Impact / Likelihood



Risks – See Appendix B for Definitions

🟢 **Technology Risk**

1 – Integrity / Availability – Solaris and Linux
2 – Integrity / Availability – Network
3 – Sensitivity / Integrity – Data Privacy
4 – Complexity / Integrity – Clarify
5 – Complexity / Integrity – SAP

🔵 **IT Process Risk**

6 – Manage SDLC – Product Design & Engineering
7 – Management Assets
8 – Manage Software Licenses
9 – Human Capital – Well Defined Roles
10 – Human Capital – Necessary Skills
11 – IT Governance
12 – Manage Support
13 – Manage Security - Add / Remove Process

🔴 **IT Projects Risk**

14 – Asia Outsourcing
15 – ITIL – Establish CMDB
16 – Consolidate IT Vendors
17 – VOIP
18 – Server Consolidation
19 – SAP Upgrades
20 – SAP Globalization
21 – Shared Service
22 – One Credence
23 – Collaboration / Workflow

⚫ **Significant Business Process**

24 – End User Computing
25 – Manufacturing
26 – Sales Order to Invoice
27 – Manage Business Continuity
28 – Executive Decision Support

Design IT Internal Audit Plan

Audit	Risks	2007	2008	2009	Beyond 2009
IT Service Management Baseline Review	(1) Integrity / Availability – Solaris and Linux, (2) Integrity / Availability – Network, (4) Complexity / Integrity – Clarify, (7) Manage Assets, (10) Human Capital – Necessary Skills, (12) Manage Support (15) ITIL – Establish CMDB		🔴		
IT Asset Management (ITAM) Baseline Review	(1) Integrity / Availability – Solaris and Linux, (2) Integrity / Availability – Network, (4) Complexity / Integrity – Clarify, (7) Manage Assets, (8) Manage Software Licenses, (10) Human Capital – Necessary Skills, (15) ITIL – Establish CMDB	🔴			🟡
Globalization Project Risk Management Review	(5) Complexity / Integrity – SAP, (20) SAP Globalization Project Risk		🔴		
Shared Service Project Controls SME	(5) Complexity / Integrity – SAP, (21) Shared Service Project Risk, (26) Sales Order to Invoice			🟡	
Outsource Manufacturing - Asia Project Controls SME	(3) Sensitivity / Integrity – Data Privacy, (4) Complexity / Integrity – Clarify, (5) Complexity / Integrity – SAP, (21) Asia Outsourcing Project Risk, (26) Manufacturing		🔴		
Data Privacy Review	(3) Sensitivity / Integrity – Data Privacy	🔴		🔴	
Business Impact Assessment	(27) Manage Business Continuity				
IT Account Management Review	(13) Manage Security		🟡		
Integrated Manufacturing Audit	(4) Complexity / Integrity – Clarify, (25) Manufacturing				🟢
Integrated SAP Audit	(5) Complexity / Integrity – SAP, (26) Sales Order to Invoice	🟡			

H High Risk M Med Risk L Low Risk

Summary

- Objectives must first be identified before risks to their achievement can be identified
- Risk is the possibility that an event will occur and adversely affect the achievement of objectives
- Consider the level of effort, your audience and your organization’s risk appetite in determining the risk assessment approach
- Understand your organization – proper context

Summary (cont.)

- To catalogue IT Risks, consider key technology applied, IT processes and IT projects
- Once complied, determine WHO will be responsible for each
- Rank – Focus on high / high
- Develop plan

Questions