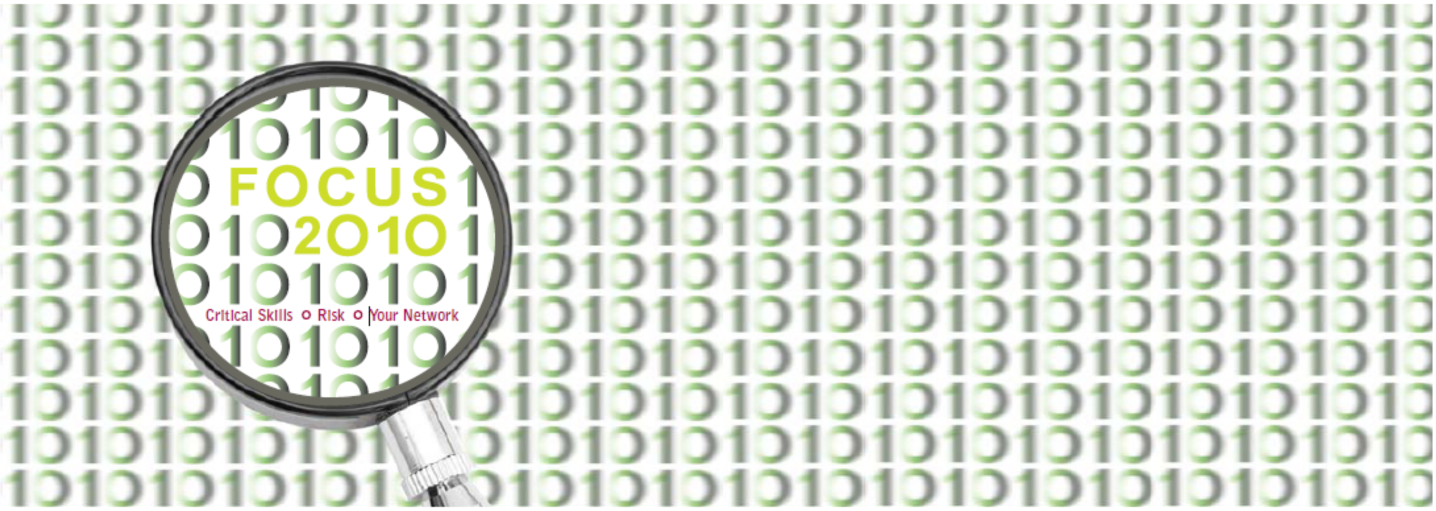
10th Annual SF ISACA Fall Conference

October 4 – 6, 2010



T23: Using Risk Portfolio Management and Self-Assessments to Mitigate Risk

Michael Zanaglio and Rajiv Agarwal,
Wells Fargo

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

Using Risk Portfolio Management and Risk Control Self Assessments to Mitigate Risk

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

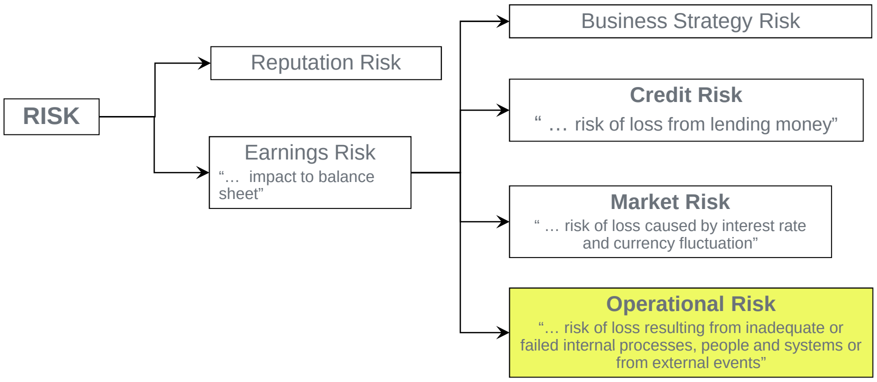
Presented By: Michael Zanaglio and Rajiv Agarwal

FOCUS 2010
Critical Skills ○ Risk ○ Your Network

Risk

- What is Risk?
  - Risk is a known or unknown event or entity that could jeopardize the achievement of an objective
- What is Operational Risk?
  - Operational Risk is the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events
    - Examples: Robberies or burglaries; Embezzlement or collusion to commit fraud; Unfair lending practices – disparate treatment; Breach of customer privacy; System failure; Human error; Vendor management

Operational Risk



RISK

Reputation Risk

Earnings Risk
"… impact to balance sheet"

Business Strategy Risk

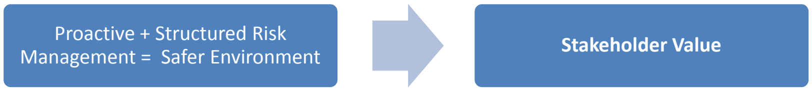
Credit Risk
" … risk of loss from lending money"

Market Risk
" … risk of loss caused by interest rate and currency fluctuation"

Operational Risk
"… risk of loss resulting from inadequate or failed internal processes, people and systems or from external events"

Operational Risk Components / Functional Risk Areas				
• Loss Management	• Human Capital	▪ Technology	▪ Financial	• Vendor
• Fiduciary	• Compliance	▪ Business Continuity	▪ Implementation Risk	• …. Others

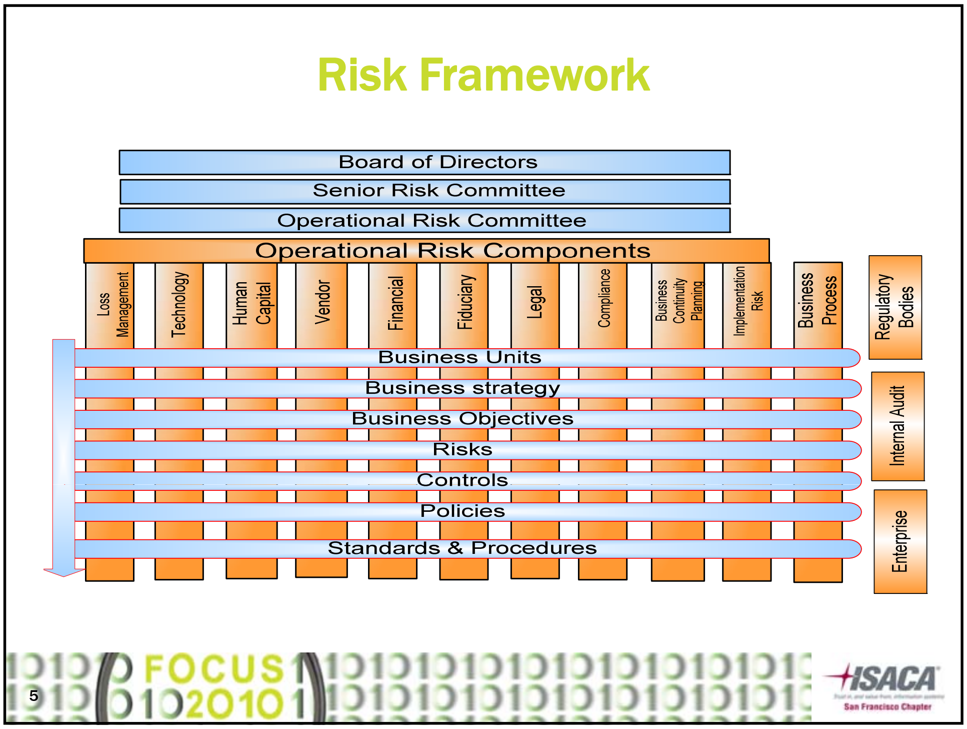
Risk Framework



Proactive + Structured Risk Management = Safer Environment

Stakeholder Value

- Systematic
- Structured
- Comprehensive Approach
- Clear Direction & Guidance
- Critical Principles, Essential Components
- Common Language
- Strategic Planning
- Implementation
- Proactive
- Key Stakeholders & Roles



Risk Framework

Board of Directors

Senior Risk Committee

Operational Risk Committee

Operational Risk Components

Loss Management

Technology

Human Capital

Vendor

Financial

Fiduciary

Legal

Compliance

Business Continuity Planning

Implementation Risk

Business Process

Regulatory Bodies

Internal Audit

Enterprise

Business Units

Business strategy

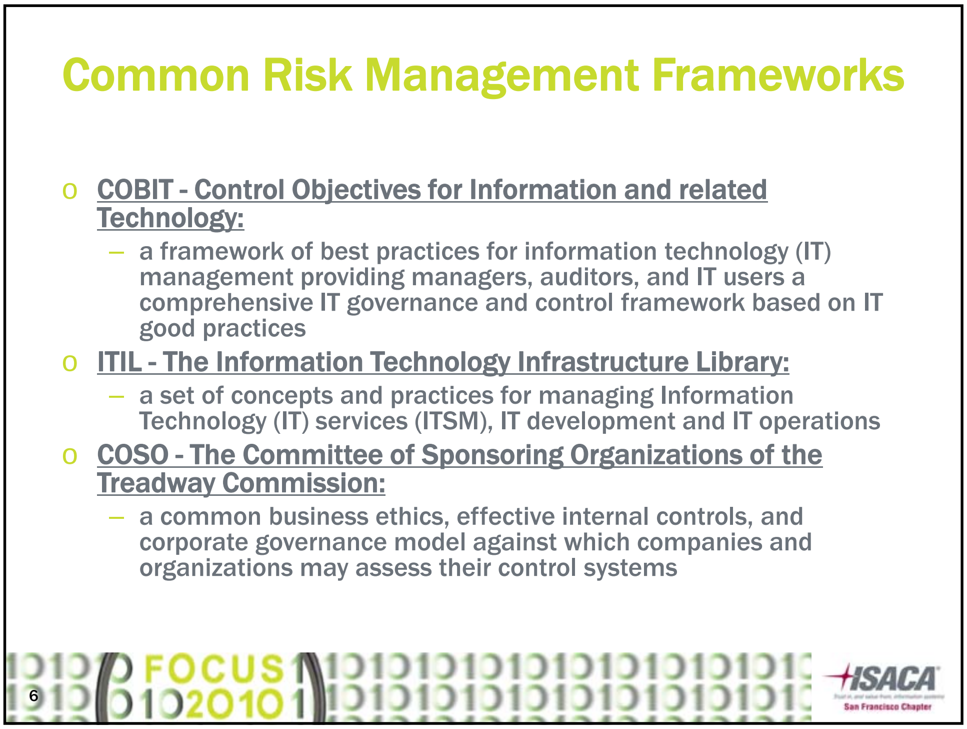
Business Objectives

Risks

Controls

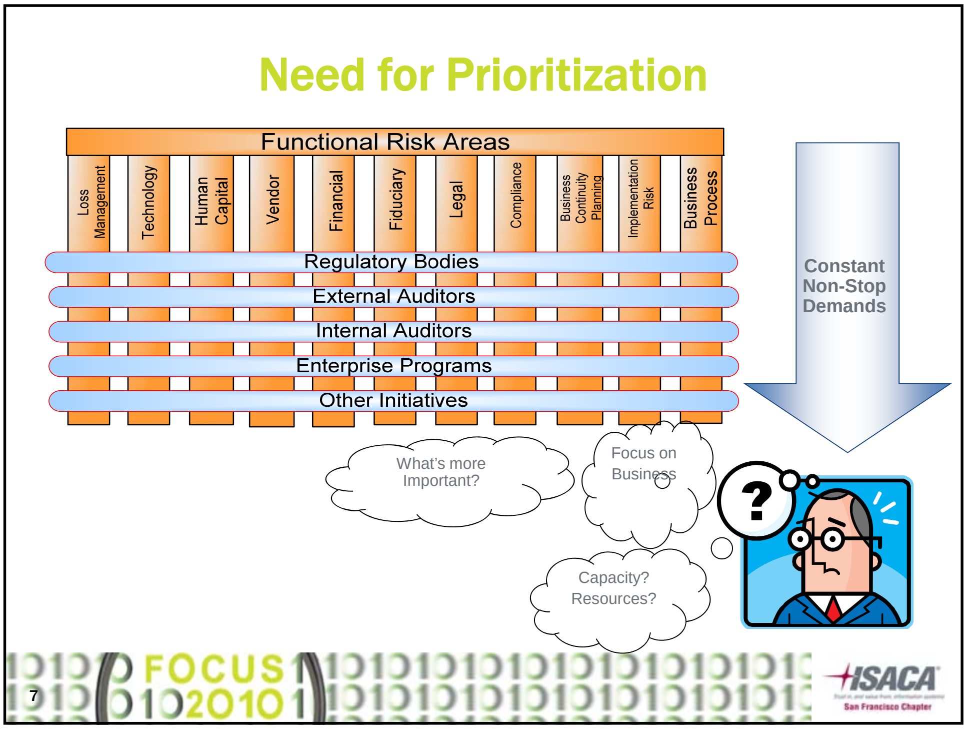
Policies

Standards & Procedures



Common Risk Management Frameworks

- **COBIT - Control Objectives for Information and related Technology:**
  - a framework of best practices for information technology (IT) management providing managers, auditors, and IT users a comprehensive IT governance and control framework based on IT good practices
- **ITIL - The Information Technology Infrastructure Library:**
  - a set of concepts and practices for managing Information Technology (IT) services (ITSM), IT development and IT operations
- **COSO - The Committee of Sponsoring Organizations of the Treadway Commission:**
  - a common business ethics, effective internal controls, and corporate governance model against which companies and organizations may assess their control systems



Need for Prioritization

Functional Risk Areas

Loss Management

Technology

Human Capital

Vendor

Financial

Fiduciary

Legal

Compliance

Business Continuity Planning

Implementation Risk

Business Process

Regulatory Bodies

External Auditors

Internal Auditors

Enterprise Programs

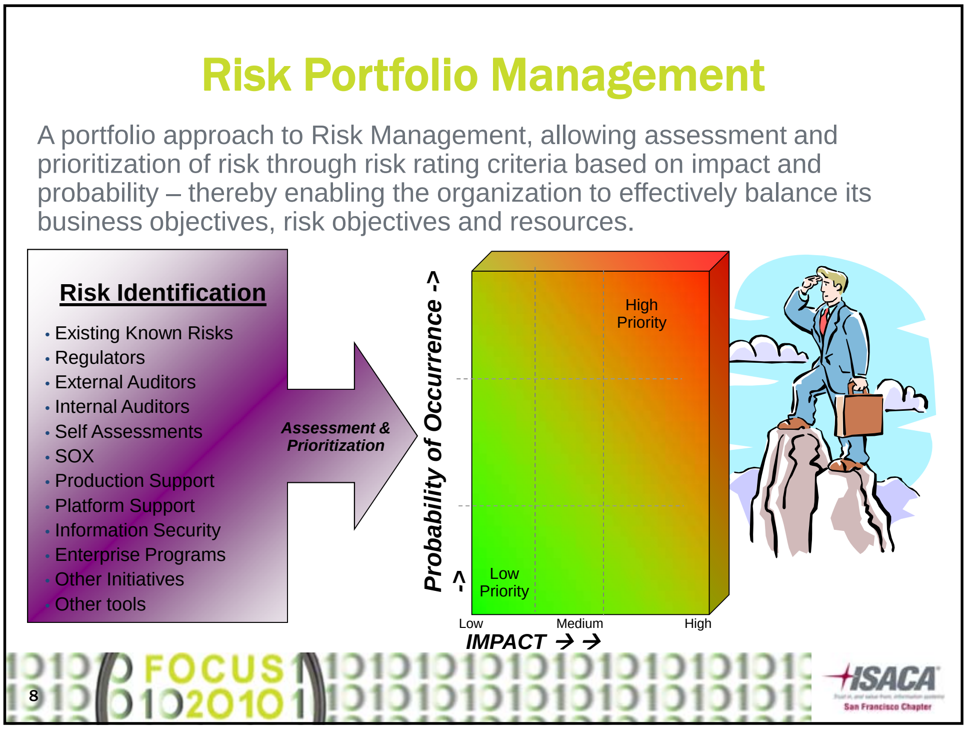
Other Initiatives

Constant Non-Stop Demands

What's more Important?

Focus on Business

Capacity? Resources?



Risk Portfolio Management

A portfolio approach to Risk Management, allowing assessment and prioritization of risk through risk rating criteria based on impact and probability – thereby enabling the organization to effectively balance its business objectives, risk objectives and resources.

Risk Identification

- Existing Known Risks
- Regulators
- External Auditors
- Internal Auditors
- Self Assessments
- SOX
- Production Support
- Platform Support
- Information Security
- Enterprise Programs
- Other Initiatives
- Other tools

Assessment & Prioritization

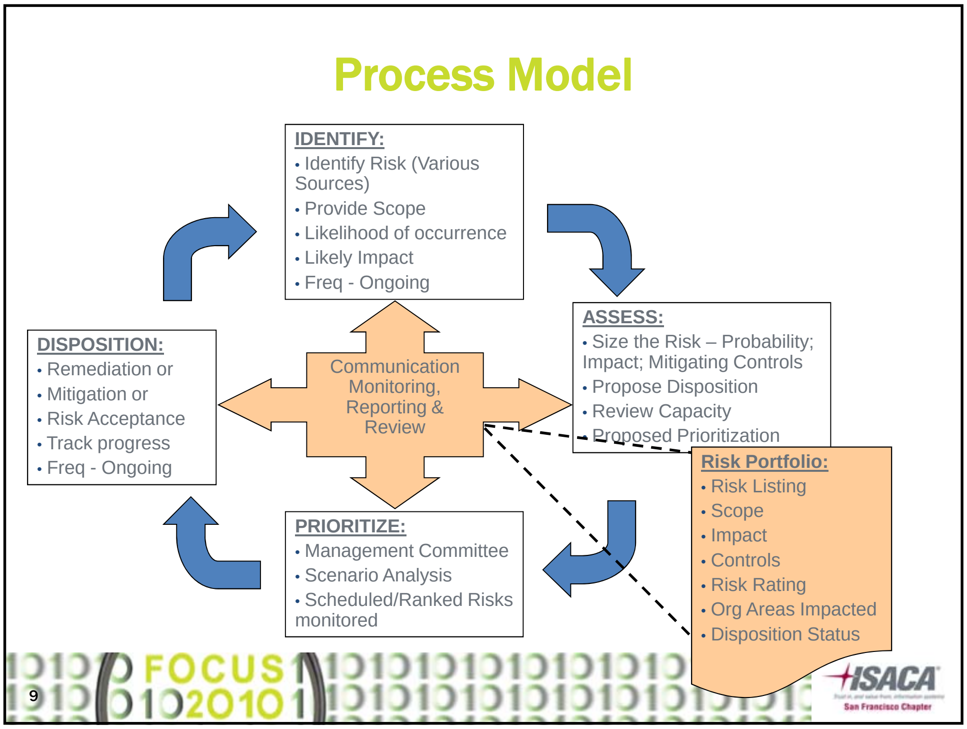
Probability of Occurrence ->

High Priority

Low Priority

Low Medium High

IMPACT → →



Process Model

IDENTIFY:
- Identify Risk (Various Sources)
- Provide Scope
- Likelihood of occurrence
- Likely Impact
- Freq - Ongoing

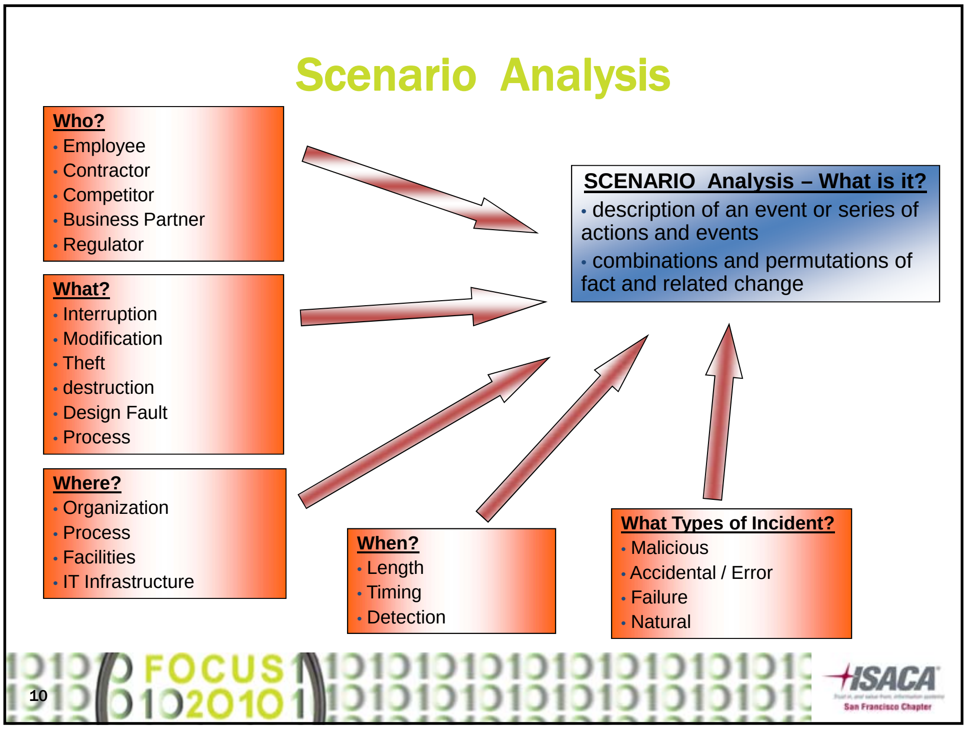
ASSESS:
- Size the Risk – Probability; Impact; Mitigating Controls
- Propose Disposition
- Review Capacity
- Proposed Prioritization

PRIORITIZE:
- Management Committee
- Scenario Analysis
- Scheduled/Ranked Risks monitored

DISPOSITION:
- Remediation or
- Mitigation or
- Risk Acceptance
- Track progress
- Freq - Ongoing

Communication Monitoring, Reporting & Review

Risk Portfolio:
- Risk Listing
- Scope
- Impact
- Controls
- Risk Rating
- Org Areas Impacted
- Disposition Status



Scenario Analysis

Who?
- Employee
- Contractor
- Competitor
- Business Partner
- Regulator

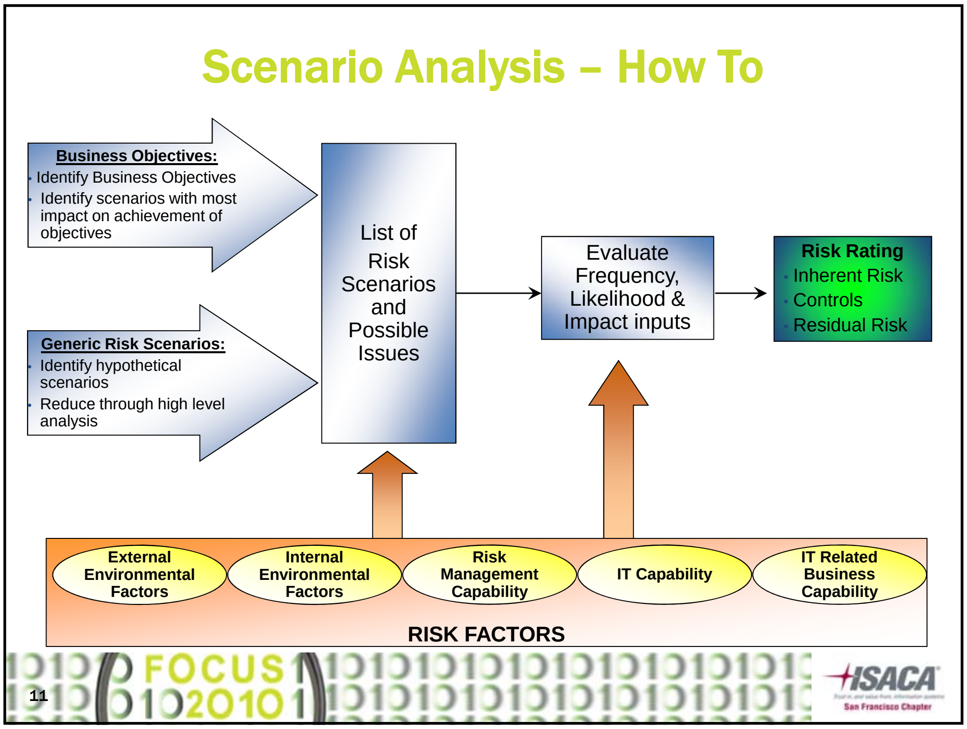
What?
- Interruption
- Modification
- Theft
- destruction
- Design Fault
- Process

Where?
- Organization
- Process
- Facilities
- IT Infrastructure

When?
- Length
- Timing
- Detection

What Types of Incident?
- Malicious
- Accidental / Error
- Failure
- Natural

SCENARIO Analysis – What is it?
- description of an event or series of actions and events
- combinations and permutations of fact and related change



Scenario Analysis – How To

Business Objectives:

- Identify Business Objectives
- Identify scenarios with most impact on achievement of objectives

Generic Risk Scenarios:

- Identify hypothetical scenarios
- Reduce through high level analysis

List of Risk Scenarios and Possible Issues

Evaluate Frequency, Likelihood & Impact inputs

Risk Rating

- Inherent Risk
- Controls
- Residual Risk

External Environmental Factors

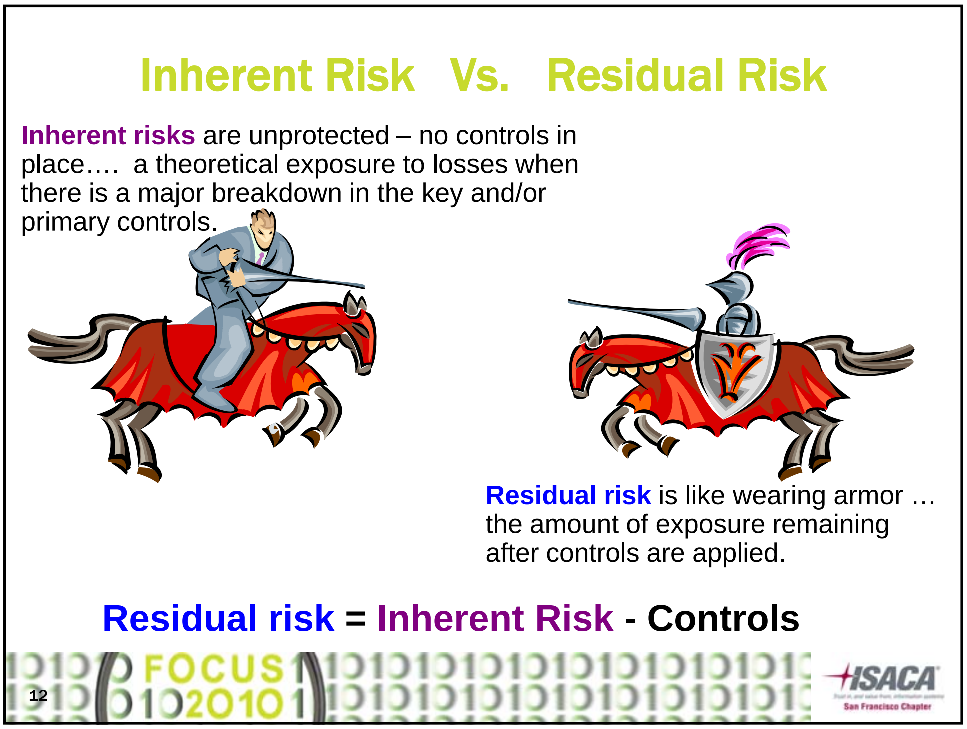
Internal Environmental Factors

Risk Management Capability

IT Capability

IT Related Business Capability

RISK FACTORS



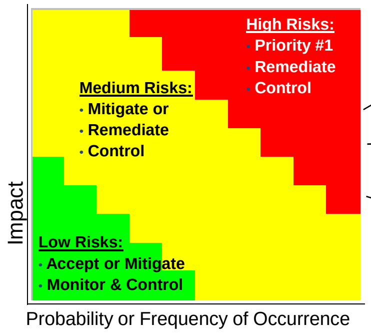
Inherent Risk Vs. Residual Risk

Inherent risks are unprotected – no controls in place…. a theoretical exposure to losses when there is a major breakdown in the key and/or primary controls.

Residual risk is like wearing armor … the amount of exposure remaining after controls are applied.

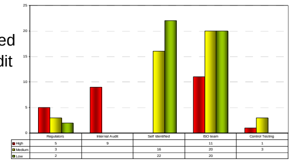
Residual risk = Inherent Risk - Controls

Risk Portfolio Analysis & Reporting



Risk Rating and Disposition will depend upon the organization's risk appetite

Examples
- Self identified
- Internal Audit
- Regulators



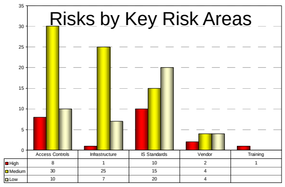
	Regulators	Internal Audit	Self Identified	ISO team	Control Testing
🟥 High	5	9		11	1
🟨 Medium	3		16	20	3
🟩 Low	2		22	20	

Heat Map by Business Units

Functional Risk Areas

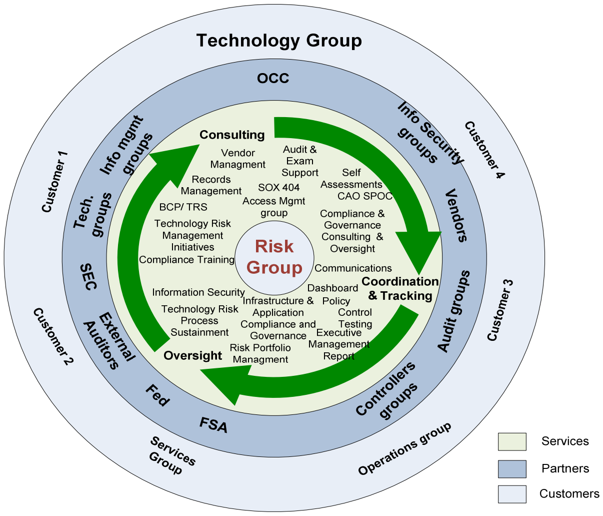
	BU1	BU2	BU3	BU4	BU5	BU6
FRA1	🟨	🟩	🟩	🟩	🟩	🟥
FRA2	🟥	🟩	🟨	🟥	🟩	🟩
FRA3	🟩	🟥	🟩	🟩	🟨	🟩
FRA4	🟩	🟩	🟩	🟩	🟩	🟩
FRA5	🟨	🟩	🟥	🟨	🟥	🟩
FRA6	🟩	🟩	🟩	🟩	🟩	🟨
FRA7	🟥	🟩	🟩	🟥	🟩	🟩
FRA8	🟩	🟩	🟨	🟩	🟩	🟩
FRA9	🟩	🟨	🟩	🟩	🟩	🟩
FRA10	🟩	🟩	🟩	🟩	🟩	🟩

Examples
- Access
- Vendor
- Infrastructure
- Information Security



	Access Controls	Infrastructure	IS Standards	Vendor	Training
🟥 High	8	1	10	2	1
🟨 Medium	30	25	15	4	
⬜ Low	10	7	20	4	

Technology Risk Management



Technology Risk Management

Management Objectives:

Information Security / Access:
- Information Security
- Access Management
- Access Engineering

Risk Identification:
- Self-Assessments
- Policy/ITOM Support
- Risk Portfolio Management

Compliance:
- SOX
- Audit & Exam Support
- BCP
- Vendor Management
- Records Management
- Compliance/Contractor Training
- Data Center Compliance

Project Management Compliance:
- Sustainment and Reporting:
- Control Testing

Executive Management Trending Report:
- Implementation Compliance Oversight

Process

Subject Matter Expert (SME) works with Business SME to define and document the following:

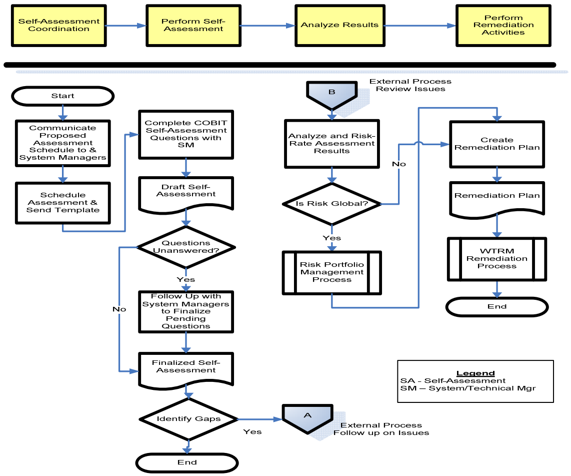
- Scope of effort
- Policies/Standards/Guidelines that apply
- Process Documentation
- Responsible/Accountable parties (RACI)
- Control Points
- Compliance Metrics/Reporting

Goals

- SOX – No significant deficiencies
- Audit – No Key issues or repeat items
- Self-Assessments and RPM – Focus on self-identification
- Single Point of Contact for all operational risk related items
- Consideration for capacity, utilization and bandwidth rates
- Proper prioritization with real business impact considered
- Consistent and accurate responses
- Oversight: Accurate and comprehensive reporting

Technology Risk Management

Self Assessment - Process Flow



Self-Assessment Coordination

Perform Self-Assessment

Analyze Results

Perform Remediation Activities

Start

Communicate Proposed Assessment Schedule to & System Managers

Schedule Assessment & Send Template

Complete COBIT Self-Assessment Questions with SM

Draft Self-Assessment

Questions Unanswered?

Yes

No

Follow Up with System Managers to Finalize Pending Questions

Finalized Self-Assessment

Identify Gaps

Yes

End

A

External Process Follow up on Issues

B

External Process Review Issues

Analyze and Risk-Rate Assessment Results

Is Risk Global?

No

Yes

Risk Portfolio Management Process

Create Remediation Plan

Remediation Plan

WTRM Remediation Process

End

Legend
SA - Self-Assessment
SM – System/Technical Mgr

Technology Risk Management

Self Assessment - Process RACI

Process Step	Self Assessment Coordination		Perform Self Assessment		Analyze Results		Remediation Activities	
R = Responsible A = Accountable C = Consulted I = Informed	Communicate Proposed Assessment Schedule to CAO, Chief of Staff & Technical Managers	Schedule Assessment	Review/ Answer COBIT-based Self Assessment Questions	Follow Up with Technical Managers & Finalize Pending	Analyze & Risk Rate Assessment Results	Institutional Risk Management Process	Create Formal Remediation Plan	Audit Remediation Process
Assessment Team	A/ R	A/ R	A/ R	A	A/ R	C	R	R
Technology Operations	I		C	I	C	A/ R	I	I
Technology Leadership	I	I		R	C	I		C
Technology Team Members	I	C		R	I	I	A	A

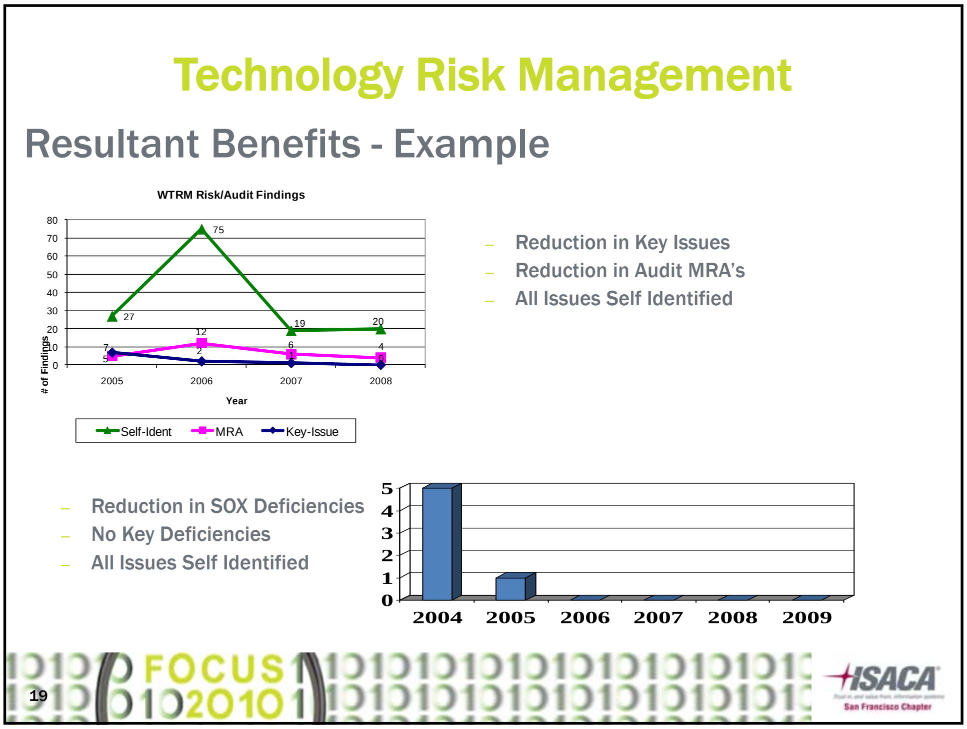
Technology Risk Management

- **Governance and Sustainment**

  The risk, audit, process and governance team conducts oversight of all compliance activities. Reports, documentation and artifacts are reviewed monthly to demonstrate adherence to process and standards. The state of compliance and is continually monitored and deviations from compliance are escalated and managed appropriately. In some cases, exceptions are identified and accepted by management based on the cost benefit analysis as well. All exceptions are monitored through closure in the future and into sustainment.

- **The Results**

  The technology risk, audit, process and governance team is accountable for the results of the ongoing risk remediation and the results. The team works within the enterprise to ensure that standards, recommended practices and risk are real and ranked to generate meaningful results for technology. All historical open key issues have been closed and satisfied, there have been Zero new key issues since the implementation of the risk, audit, process and governance process and the self identified items increased and have been resolved to satisfaction through real residual risk mitigation.

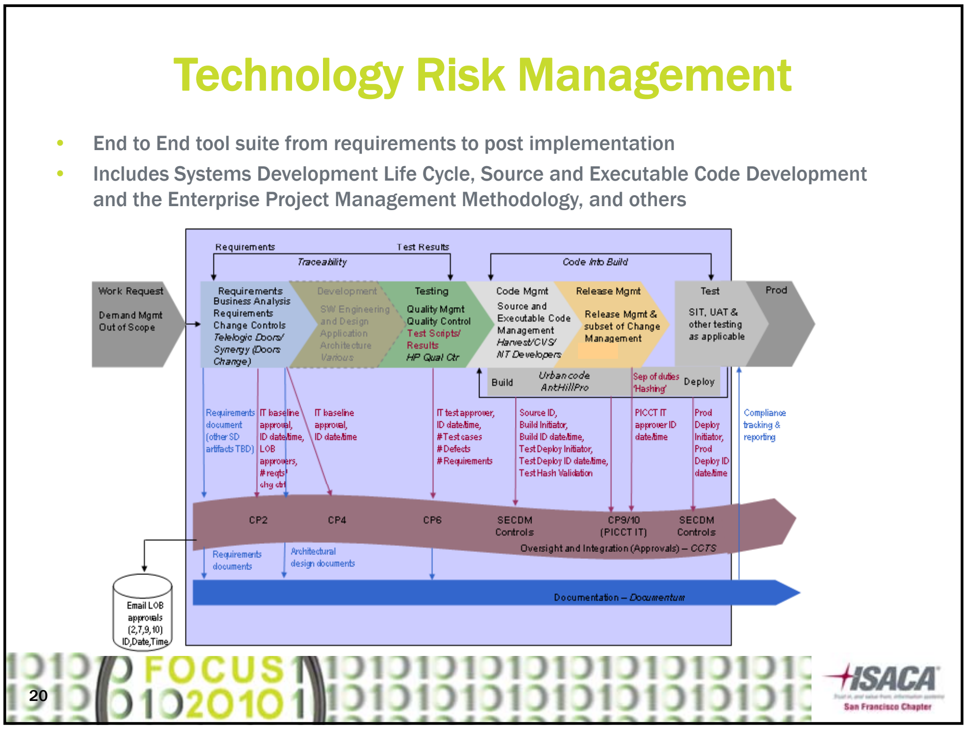


Technology Risk Management

Resultant Benefits - Example

- Reduction in Key Issues
- Reduction in Audit MRA's
- All Issues Self Identified

- Reduction in SOX Deficiencies
- No Key Deficiencies
- All Issues Self Identified



Technology Risk Management

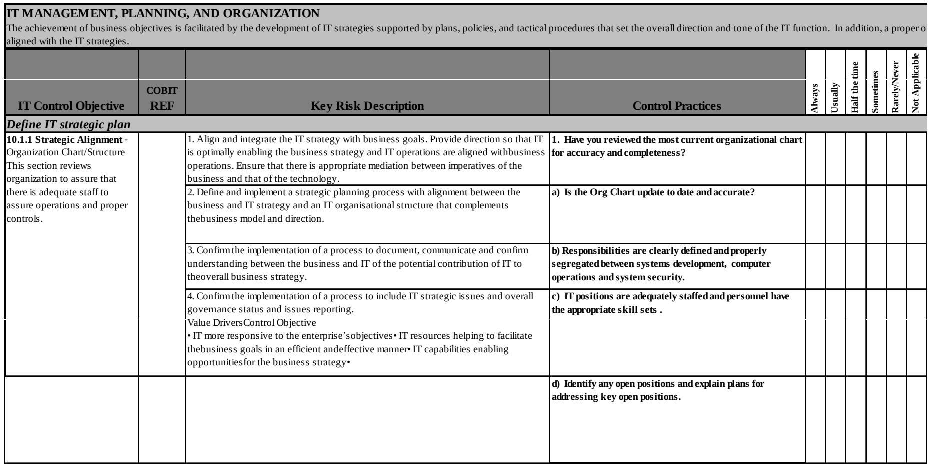
- End to End tool suite from requirements to post implementation
- Includes Systems Development Life Cycle, Source and Executable Code Development and the Enterprise Project Management Methodology, and others

Technology Risk Management

PROCESS	COMPONENTS	GOAL	SUSTAINABLE
Self- Assessment	Annual Review	No Key Audit Findings	Yes
Audit Mgt	SPOC for audit partners	No Key Issues	Yes
Audit Remediation	Issue identification, milestones, evidence for closure	No missed dates, Risk Mitigated	Yes
Sox	Quarterly testing	No deficiencies	Yes
Project Compliance	PLC, EPMM, PMO, IRB, AWM	Artifacts completed and accurate	Yes
Inventory Mgt	PICCT, EDBI, DSDMB	Accuracy of system of record	Enterprise dependent
Inventory Compliance	Database compliance, Compliance Checker, KEON	Regular review and reporting	Enterprise dependent
Code Change Mgt	PICCT, SDLC, SECDM, QM	Code mgt, sep of duties, approvals	Yes
Access Mgt	ISR3, DBMS, ACP, SOD, CIS	Proper access controls	Enterprise dependent
TRS	ARP, IRP, DCPR	Recover apps, db's, servers	Yes
Problem Mgt	PICCT, Incident Mgt	Quick resolution of business impact	Yes
Vendor	Contracts, Frictionless, SLA, SAS70	Process, documentation, control practices	Yes
CIS	Standards, ASRAT	Standards adherence	Yes
BCP	LDRPS	Personnel Safety and continuity of business	Yes
AML, Basel, M&A	Enterprise Projects and Processes	Compliance	Yes

Technology Risk Management

Self Assessment Sample Format



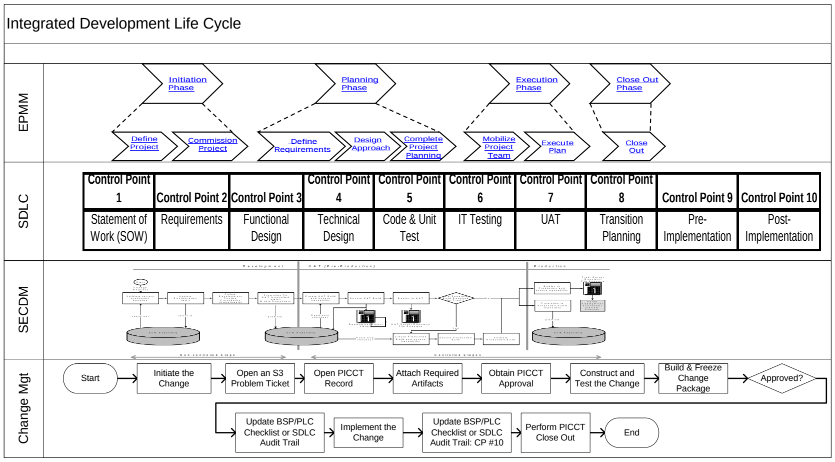
IT MANAGEMENT, PLANNING, AND ORGANIZATION

The achievement of business objectives is facilitated by the development of IT strategies supported by plans, policies, and tactical procedures that set the overall direction and tone of the IT function. In addition, a proper o aligned with the IT strategies.

IT Control Objective	COBIT REF	Key Risk Description	Control Practices	Always	Usually	Half the time	Sometimes	Rarely/Never	Not Applicable
Define IT strategic plan									
10.1.1 Strategic Alignment - Organization Chart/Structure This section reviews organization to assure that there is adequate staff to assure operations and proper controls.		1. Align and integrate the IT strategy with business goals. Provide direction so that IT is optimally enabling the business strategy and IT operations are aligned withbusiness operations. Ensure that there is appropriate mediation between imperatives of the business and that of the technology.	**1. Have you reviewed the most current organizational chart for accuracy and completeness?**						
		2. Define and implement a strategic planning process with alignment between the business and IT strategy and an IT organisational structure that complements thebusiness model and direction.	**a) Is the Org Chart update to date and accurate?**						
		3. Confirm the implementation of a process to document, communicate and confirm understanding between the business and IT of the potential contribution of IT to theoverall business strategy.	**b) Responsibilities are clearly defined and properly segregated between systems development, computer operations and system security.**						
		4. Confirm the implementation of a process to include IT strategic issues and overall governance status and issues reporting. Value DriversControl Objective • IT more responsive to the enterprise'sobjectives• IT resources helping to facilitate thebusiness goals in an efficient andeffective manner• IT capabilities enabling opportunitiesfor the business strategy•	**c) IT positions are adequately staffed and personnel have the appropriate skill sets .**						
			d) Identify any open positions and explain plans for addressing key open positions.						

Technology Risk Management

Strategy – Integrate Existing Development Sub-processes

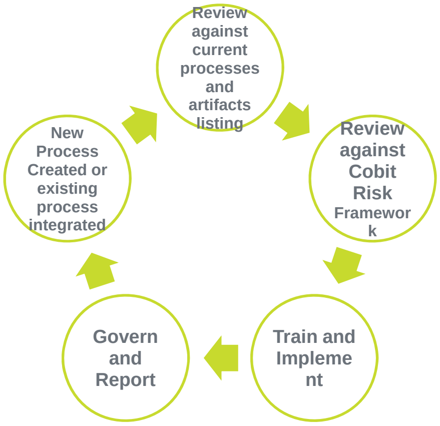


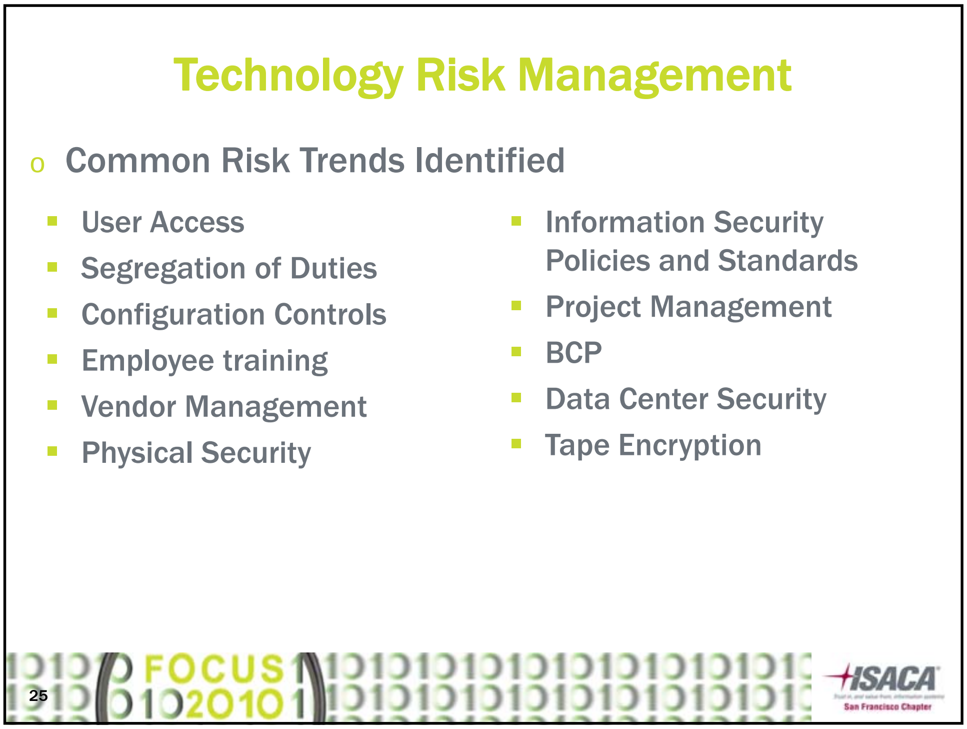
Control Point 1	Control Point 2	Control Point 3	Control Point 4	Control Point 5	Control Point 6	Control Point 7	Control Point 8	Control Point 9	Control Point 10
Statement of Work (SOW)	Requirements	Functional Design	Technical Design	Code & Unit Test	IT Testing	UAT	Transition Planning	Pre-Implementation	Post-Implementation

Technology Risk Management

Strategy – Process Review and Integration

- Review current processes for effort or artifact duplication
- Review current processes and artifacts against COBIT and Enterprise Risk to identify gaps or redundancy
- Create dashboard to report on process health across technology
- Process integration managed by process team
- Process governance either monitored through existing control points or reviewed by technology governance team
- Training plan created based on process improvement needs


Review against current processes and artifacts listing
Review against Cobit Risk Framewor k
Train and Impleme nt
Govern and Report
New Process Created or existing process integrated

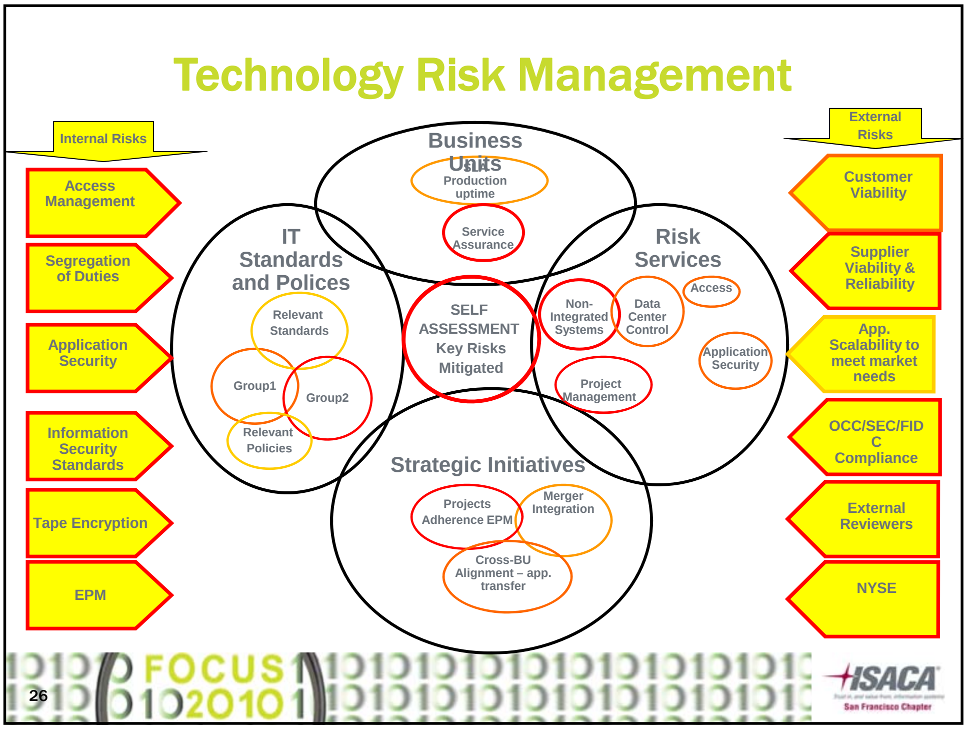


Technology Risk Management

- Common Risk Trends Identified
  - User Access
  - Segregation of Duties
  - Configuration Controls
  - Employee training
  - Vendor Management
  - Physical Security
  - Information Security Policies and Standards
  - Project Management
  - BCP
  - Data Center Security
  - Tape Encryption

FOCUS 2010

ISACA San Francisco Chapter



Technology Risk Management

Internal Risks

Access Management

Segregation of Duties

Application Security

Information Security Standards

Tape Encryption

EPM

Business Units

SLA Production uptime

Service Assurance

IT Standards and Polices

Relevant Standards

Group1

Group2

Relevant Policies

SELF ASSESSMENT Key Risks Mitigated

Risk Services

Access

Non-Integrated Systems

Data Center Control

Application Security

Project Management

Strategic Initiatives

Projects Adherence EPM

Merger Integration

Cross-BU Alignment – app. transfer

External Risks

Customer Viability

Supplier Viability & Reliability

App. Scalability to meet market needs

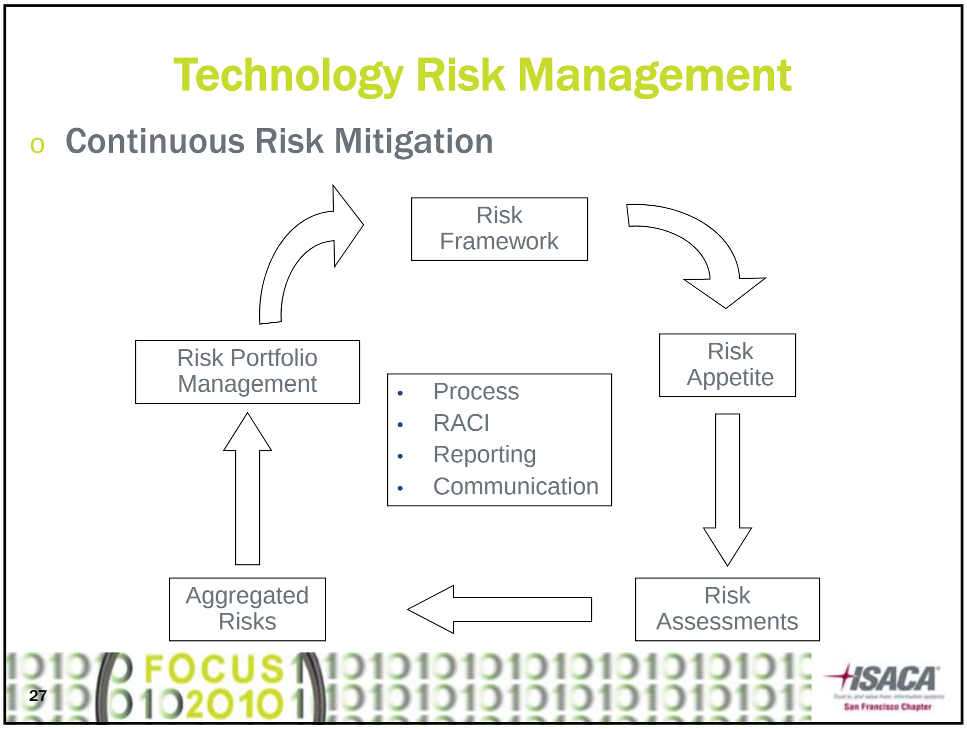
OCC/SEC/FIDC Compliance

External Reviewers

NYSE

FOCUS 2010

ISACA San Francisco Chapter



Technology Risk Management

- Continuous Risk Mitigation

Risk Framework

Risk Appetite

Risk Assessments

Aggregated Risks

Risk Portfolio Management

- Process
- RACI
- Reporting
- Communication