

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



Presented By: Michael Zanaglio and Rajiv Agarwal

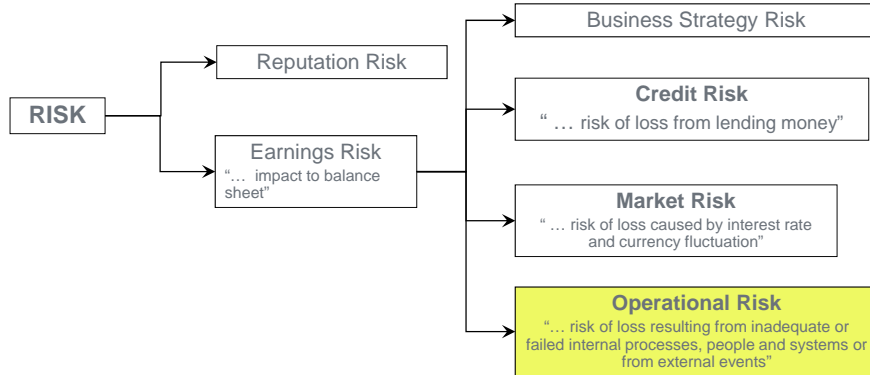


Risk

- 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



Operational Risk Components / Functional Risk Areas

• Loss Management	• Human Capital	• Technology	• Financial	• Vendor
• Fiduciary	• Compliance	• Business Continuity	• Implementation Risk	• Others

3



Risk Framework

Proactive + Structured Risk Management = Safer Environment



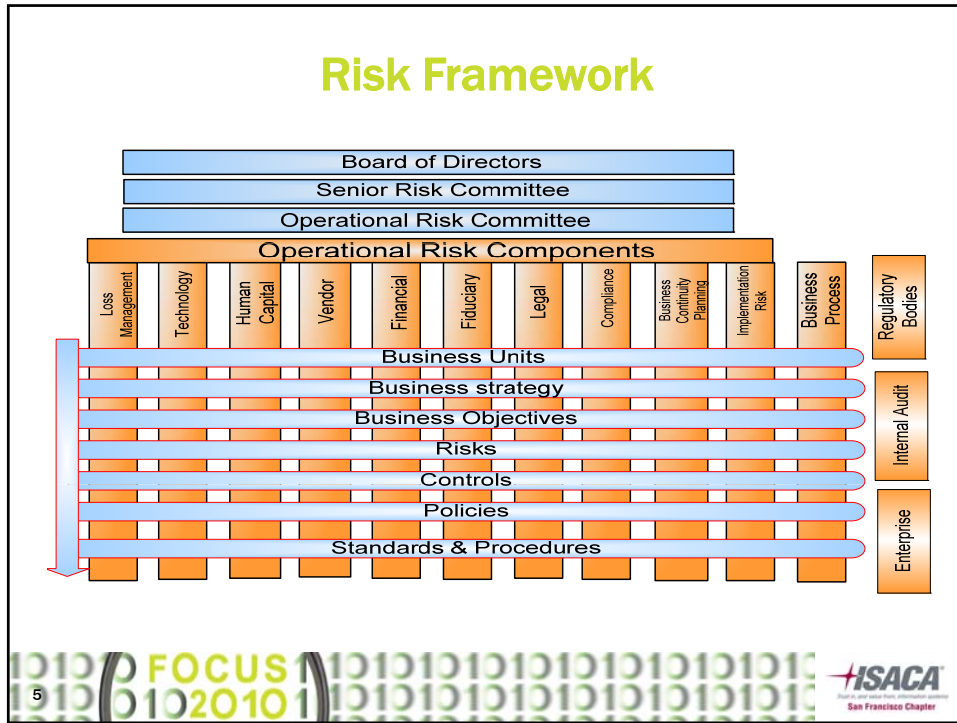
Stakeholder Value

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

4



Risk Framework



Common Risk Management Frameworks

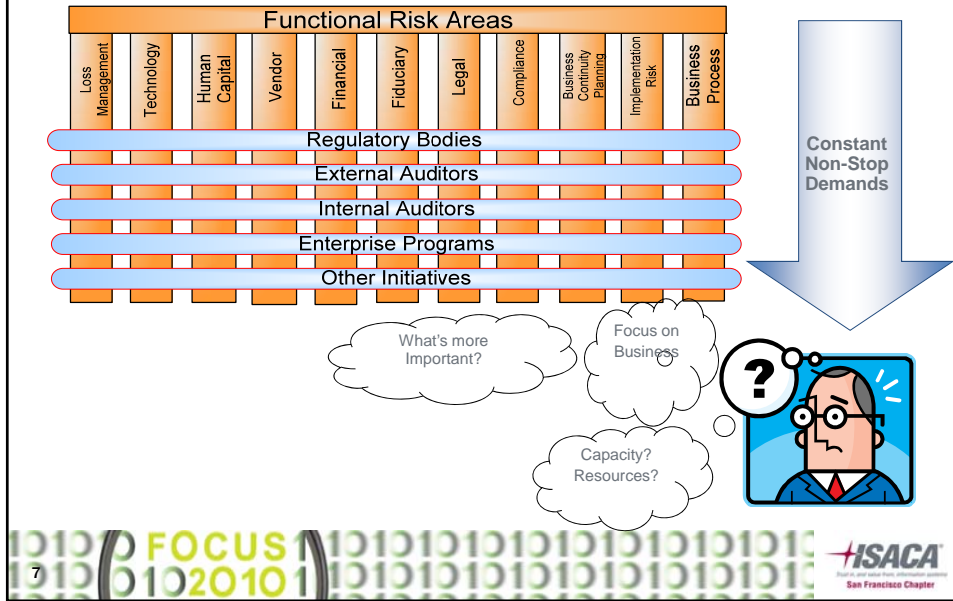
- **COBIT - Control Objectives for Information and related Technology:**
 - a framework of best practices for information technology (IT) management providing managers, auditors, and IT users a comprehensive IT governance and control framework based on IT good practices
- **ITIL - The Information Technology 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

5

6

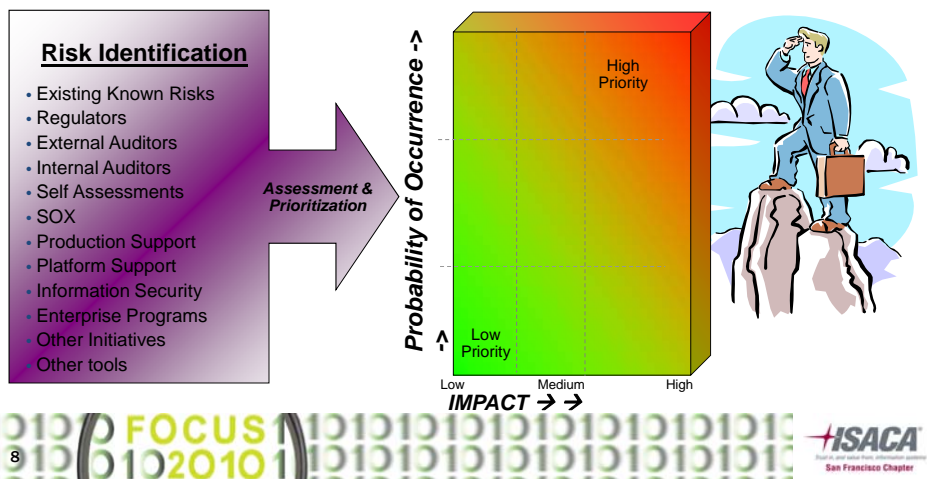
ISACA
Institute of Information Systems Auditors and Accountants
San Francisco Chapter

Need for Prioritization

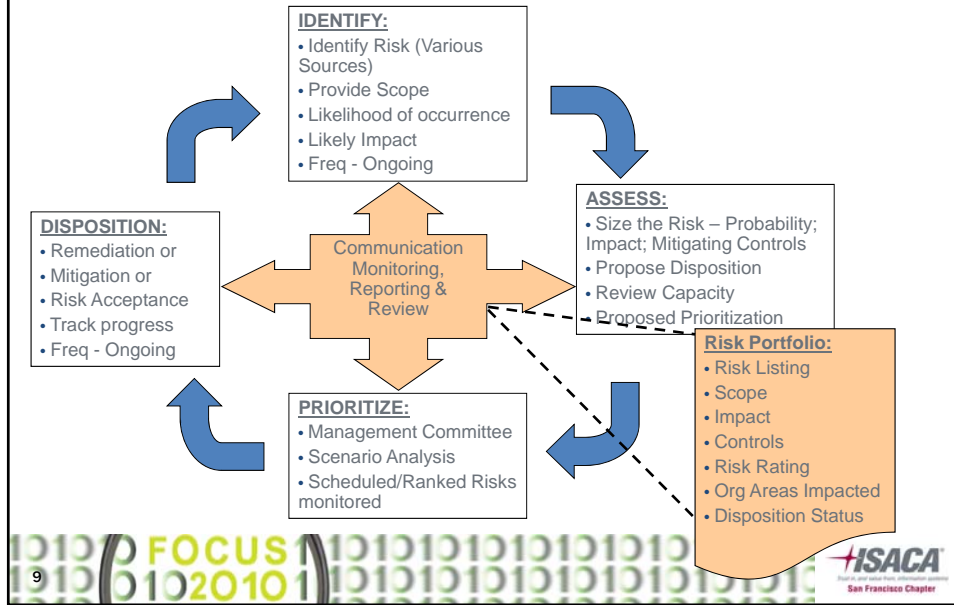


Risk Portfolio Management

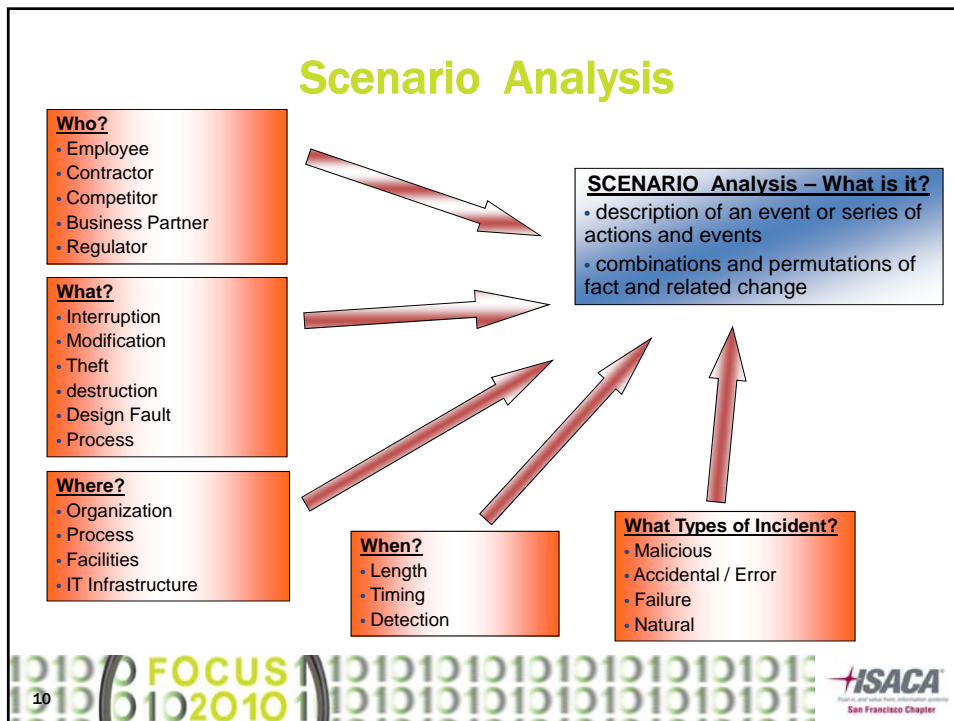
A portfolio approach to Risk Management, allowing assessment and prioritization of risk through risk rating criteria based on impact and probability – thereby enabling the organization to effectively balance its business objectives, risk objectives and resources.



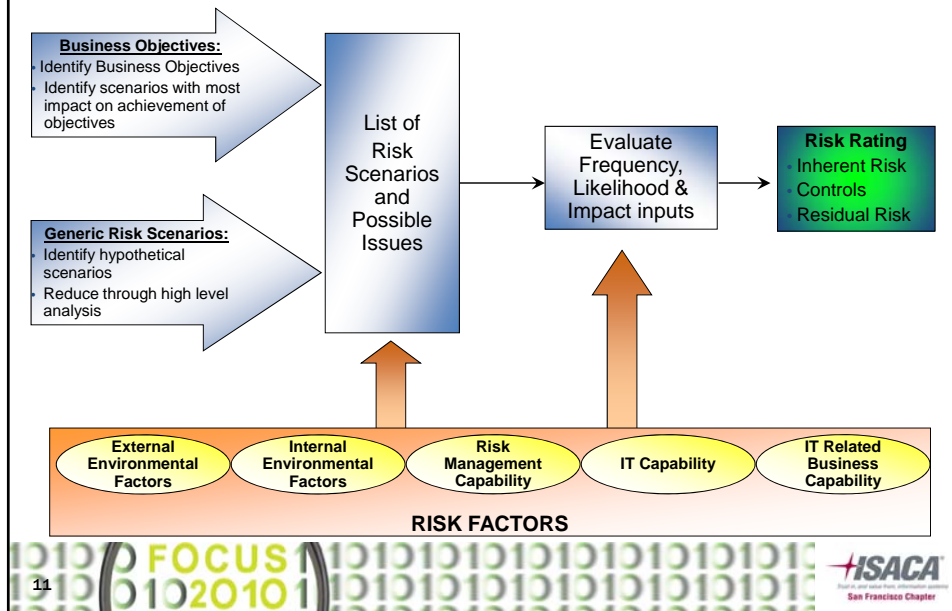
Process Model



Scenario Analysis



Scenario Analysis – How To



Inherent Risk Vs. Residual Risk

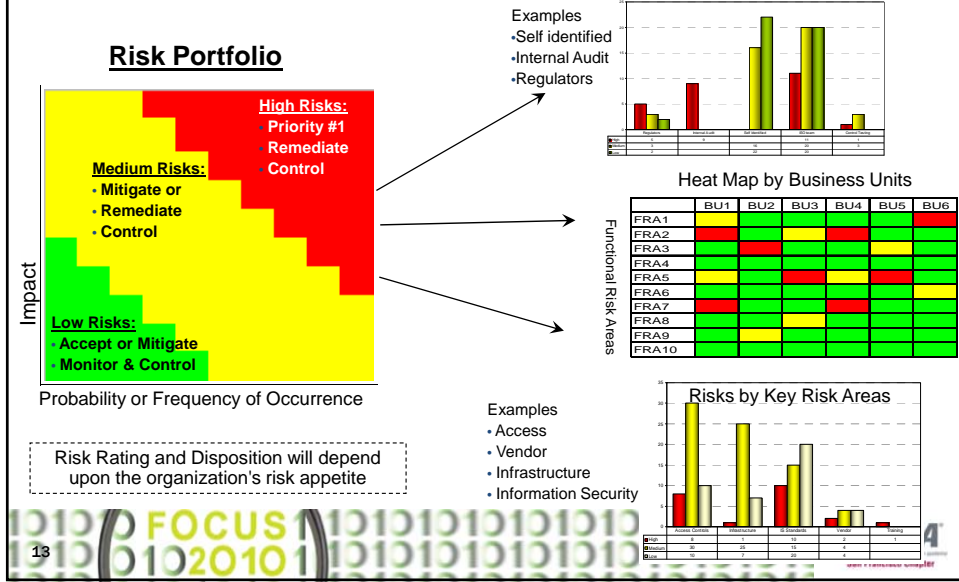
Inherent risks are unprotected – no controls in place.... a theoretical exposure to losses when there is a major breakdown in the key and/or primary controls.



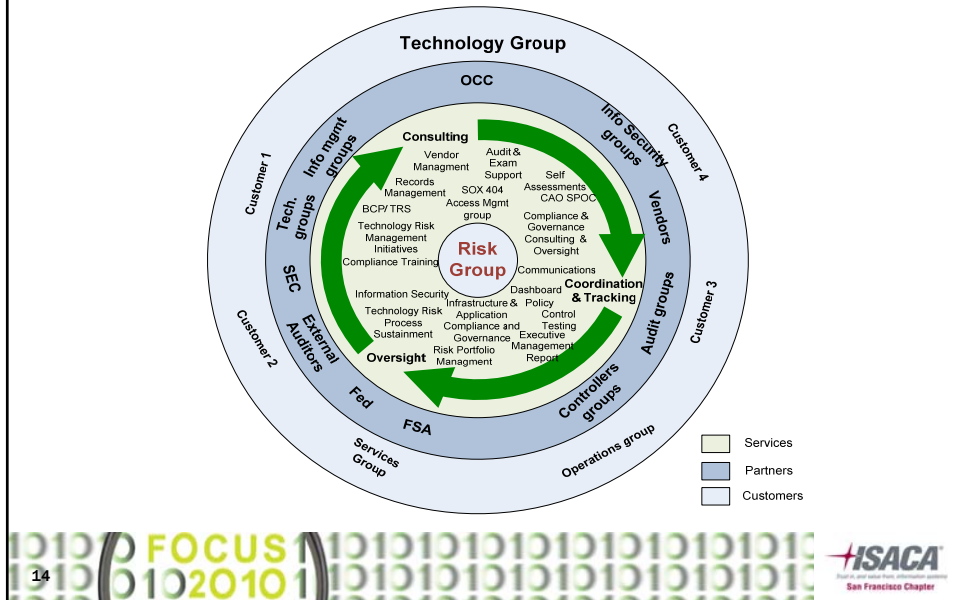
Residual risk is like wearing armor ... the amount of exposure remaining after controls are applied.

Residual risk = Inherent Risk - Controls

Risk Portfolio Analysis & Reporting



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

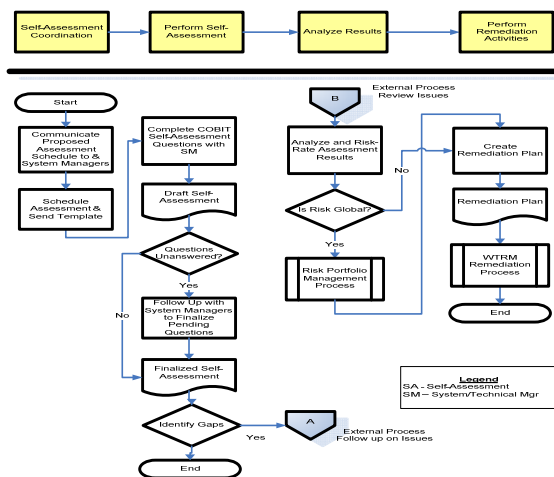
Goals

- 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



Technology Risk Management

Self Assessment - Process RACI

Process Step	Self Assessment Coordination		Perform Self Assessment		Analyze Results		Remediation Activities	
	Communicate Proposed Assessment Schedule to CIO, 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
R = Responsible A = Accountable C = Consulted I = Informed								
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.

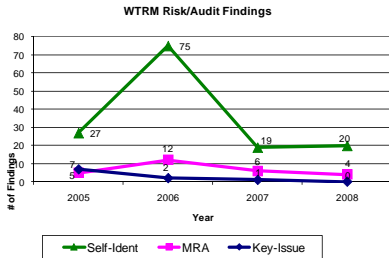
- The Results

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.



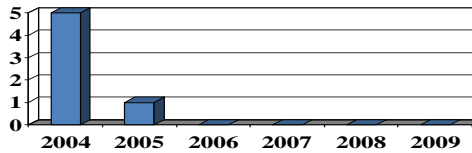
Technology Risk Management

Resultant Benefits - Example



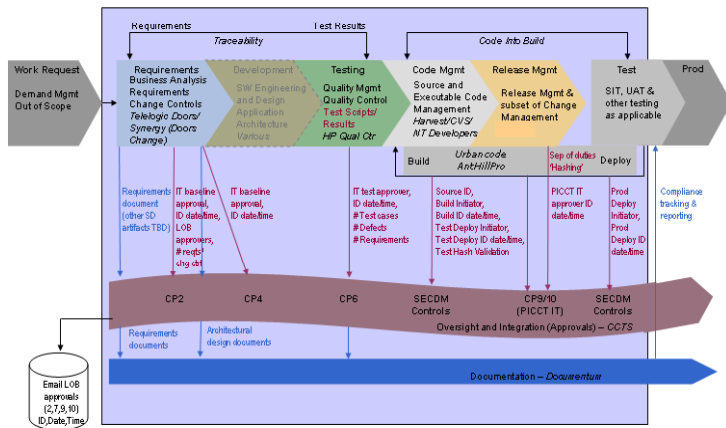
- Reduction in Key Issues
- Reduction in Audit MRA's
- All Issues Self Identified

- 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

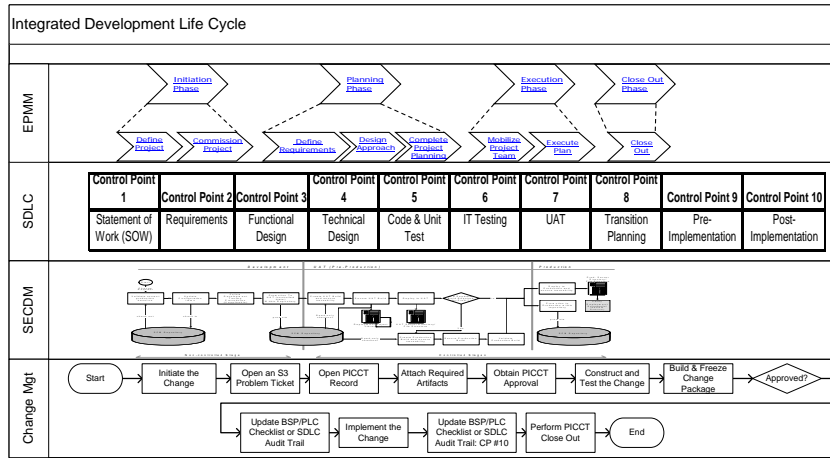
IT MANAGEMENT, PLANNING, AND ORGANIZATION
 The achievement of business objectives is facilitated by the development of IT strategies supported by plans, policies, and tactical procedures that set the overall direction and tone of the IT function. In addition, a proper aligned with the IT strategies.

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 with business 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? a) Is the Org Chart update to date and accurate?						
		2. Define and implement a strategic planning process with alignment between the business and IT strategy and an IT organizational structure that complements the business model and direction.	b) Responsibilities are clearly defined and properly segregated between systems development, computer operations and system security.						
		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 the overall business strategy.	c) IT positions are adequately staffed and personnel have the appropriate skill sets .						
		4. Confirm the implementation of a process to include IT strategic issues and overall governance status and issues reporting. Value Drivers/Control Objective • IT more responsive to the enterprise's objectives • IT resources helping to facilitate the business goals in an efficient and effective manner • IT capabilities enabling opportunities for the business strategy	d) Identify any open positions and explain plans for addressing key open positions.						



Technology Risk Management

Strategy – Integrate Existing Development Sub-processes



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

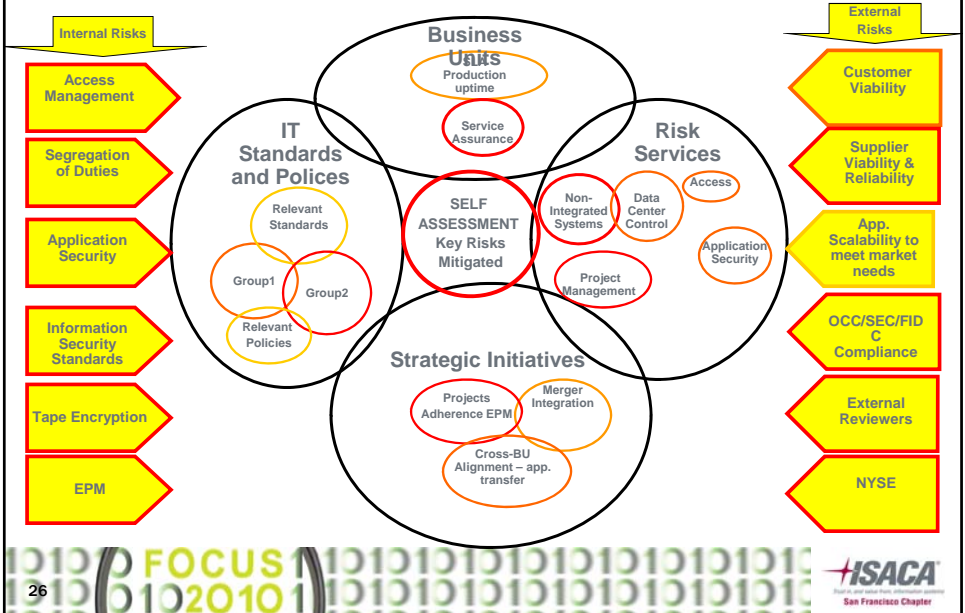


Technology Risk Management

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

Technology Risk Management



Technology Risk Management

- Continuous Risk Mitigation

