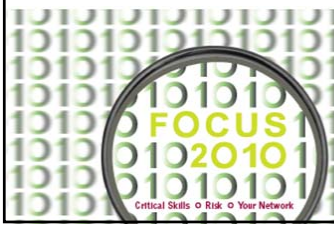
ISACA
Trust in, and value from, information systems
San Francisco Chapter

Conducting Enterprise-Wide IT Risk Assessments

Session S-11

Monday, October 4, 2010
(10:15am-11:45am)

Presented by...
Lance M. Turcato, CGEIT, CISA, CISM, CPA, CITP



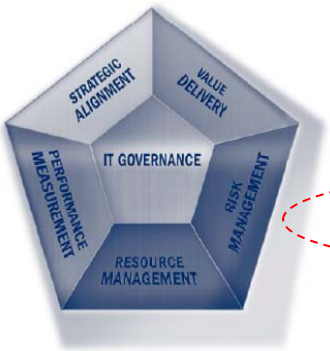
Agenda

- IT Governance Focus Area (Risk Management)
- IT Governance Frameworks (*Risk* IT)
- General IT Risk Assessment Phases
- Scoring Criteria – Factors to Consider
- Compiling IT Risk Assessment Results
- Leveraging the IT Risk Assessment in Audit Planning
- Ongoing and Annual Updates
- City-wide IT Risk Assessments @ City of Phoenix

IT Governance (ITG)

GOVERNANCE INSTITUTE

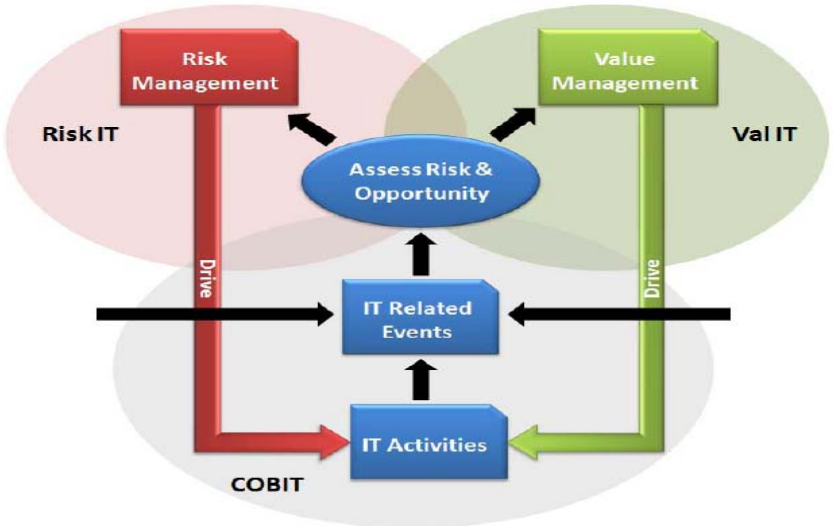
IT Governance Focus Areas



- Strategic Alignment
- Value Delivery
- Risk Management
- Resource Management
- Performance Measurement

FOCUS 2010 ISACA San Francisco Chapter

Three ITGI Frameworks
Risk IT ™ , *Val*IT ™ , CobiT ™



FOCUS 2010 ISACA San Francisco Chapter

Risk Management

- **Value Delivery** = creation of value
- **Risk Management** = preservation of value

ISO/IEC 38500
Principle 5
(Conformance)

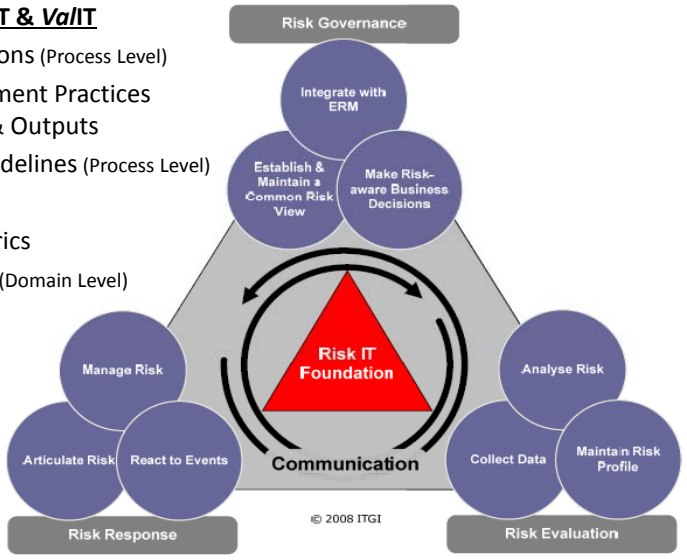
Risk Management Elements

- Final ***responsibility*** rests with the board
- ***Transparency*** about the significant risks
- Risk management ***embedded*** in enterprise operations (Integrated risk management)
- Internal ***Control Framework***
- ***Proactive*** risk management creates competitive advantage
- Continuous process (risk identification, risk mitigation, acceptance of residual risk)

Risk Management
Risk IT™ (Risk Components)

Consistent with COBIT & *Val*IT

- Process Descriptions (Process Level)
  - Key Management Practices with Inputs & Outputs
- Management Guidelines (Process Level)
  - RACI Charts
  - Goals & Metrics
- Maturity Models (Domain Level)



General IT Risk Assessment Phases

1. Inventory Process / Environment Understanding
2. Departmental Self-Assessments
3. Departmental Risk Evaluations
4. Evaluation of Overall IT Risk Profile
5. Compiling Results

IT Risk Assessment Phases
Inventory Process

- Business Processes
- Applications
- Systems
- Leveraging Existing and Prior Inventories

IT Risk Assessment Phases
Departmental Self-Assessments

- Departmental Control
- Departmental System Infrastructures
- Departmental Applications

IT Risk Assessment Phases
Departmental Risk Evaluations

- Validation of Controls
- Validation of Inventories
- Inquiry and Observation

IT Risk Assessment Phases
IT Risk Profile & Results

- Evaluation of overall ***IT Risk Profile***
- Compiling Results
  - Database Repository
  - Enterprise-wide Risk Factors

Scoring Criteria

- Dimensions of Risk
  - Sensitivity / Confidentiality
  - Integrity
  - Availability
  - Project
  - Fraud
  - Organization-specific (e.g., Public Safety)

Scoring Criteria
Continued

- Magnitude & Probability (high, med, low)
- Inherent Risk
- Estimated Residual Risk
  - Impact of internal controls on residual risk
- Score Calculation / Algorithms
- Aggregate Risk Score

Compiling IT Risk Assessment Results

- Enterprise-wide High-Level Risks
- Localized High-Level Risks
- Departmental Risk Scores
- System-specific Risk Scores
- Prioritization
- Reporting

Defining IT Audit Plans
Leveraging the IT Risk Assessment Results

- Defining the "IT Audit Universe"
- Multi-Year (rotational) Plans
- Annual Plans
- Individual Audit Plans

Ongoing & Annual Updates

- Risk Assessment (a point in time analysis)
- Importance of Ongoing / Annual Updates
- Departmental Risk Update Schedules
- Integration with IT Strategic Planning

City-wide IT Risk Assessments at...

City of Phoenix

What's Unique about Public Sector?

Private Sector (for profit)	- vs -	Public Sector (Not-for-Profit)
Profit **Motivation**	**A.**	"Efficiency" Motivation
Clearer hierarchical **accountability** environments	**B.**	More complex, political accountability environments
More flexibility to decide & to **execute quickly**	**C.**	Less flexibility to decide & execute quickly
Board/Shareholder **exposure/oversight**	**D.**	Board + More intense public exposure/oversight
Limits on required information **disclosure**	**E.**	Freedom of Information Acts / dictated disclosure
Higher tolerance of **discretionary spending** – less demand for full fiscal transparency	**F.**	More limited tolerance for discretionary spending and more demand for full fiscal transparency
Management often has more ability to effect **cultural change** within their span of control	**G.**	Difficult to effect significant cultural change and make it "stick" long-term – even within a span of control
Most products and services are delivered in a fully **competitive market place**	**H.**	Most products & services are delivered to regulated markets that are less-than fully-competitive
Customers "vote with their feet" & "wallets"	**I.**	Customer has limited choices re: product/services

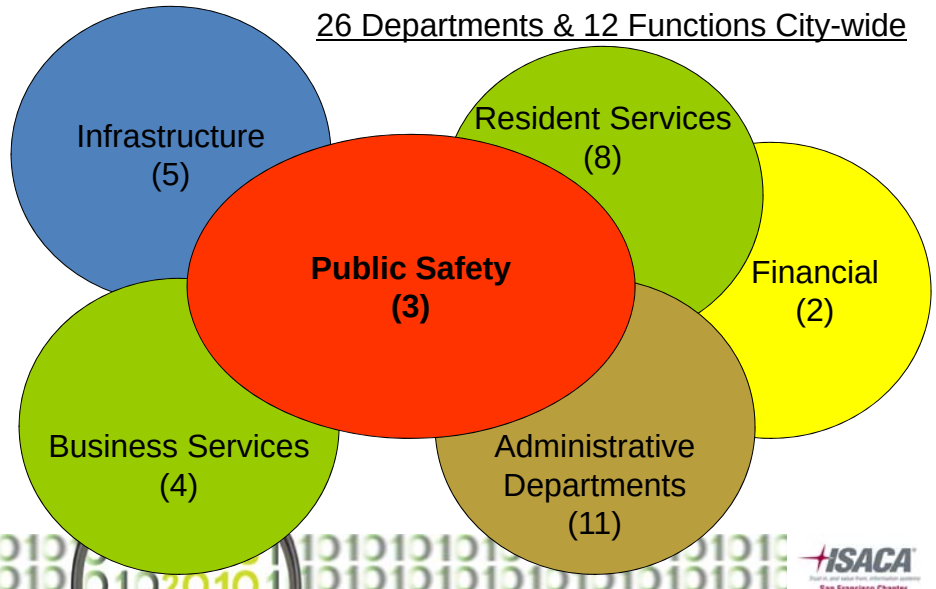
Phoenix, Arizona - Trivia

- Incorporated February 25, 1881
- 5th Largest City in the USA:
  - Largest city in the American Southwest and Mountain time zones
  - Second largest city in the Western US after Los Angeles
  - Only state capital with population > 1 million
- Estimated Population:
  - City of Phoenix = 1,552,259 (Phoenix Metro Area = 4,179,427)
- National & International Awards:
  - "Best-run City Government in the World" (Carl Bertelsmann Foundation Award - Germany)
  - "Best-Managed City" (Governing Magazine)
  - "A" Rating
    - Phoenix was the only city among the nation's 35 largest urban centers to earn an overall grade of "A." Year long, in-depth study of management efficiency by Maxwell School of Citizenship and Public Affairs, Syracuse University

A Highly Diverse Enterprise

City of Phoenix

26 Departments & 12 Functions City-wide



City "*Lines of Business*"

City of Phoenix

Public Safety
- Police
- Fire
- Municipal Court

Infrastructure
- Aviation
- Streets
- Engineering
- Planning
- Public Transit

Resident Services
- Human Services
- Neighborhood Services
- Housing
- Library
- Parks & Recreation
- Water
- Public Works
- City Manager Functions (Family Advocacy, etc.)

Administrative
- IT Services (ITS)
- Personnel
- City Clerk
- Finance
- Budget & Research
- City Attorney
- Retirement
- Equal Opportunity
- Public Information Office
- Intergovernmental Programs
- City Auditor

Financial
- Finance
- Budget & Research

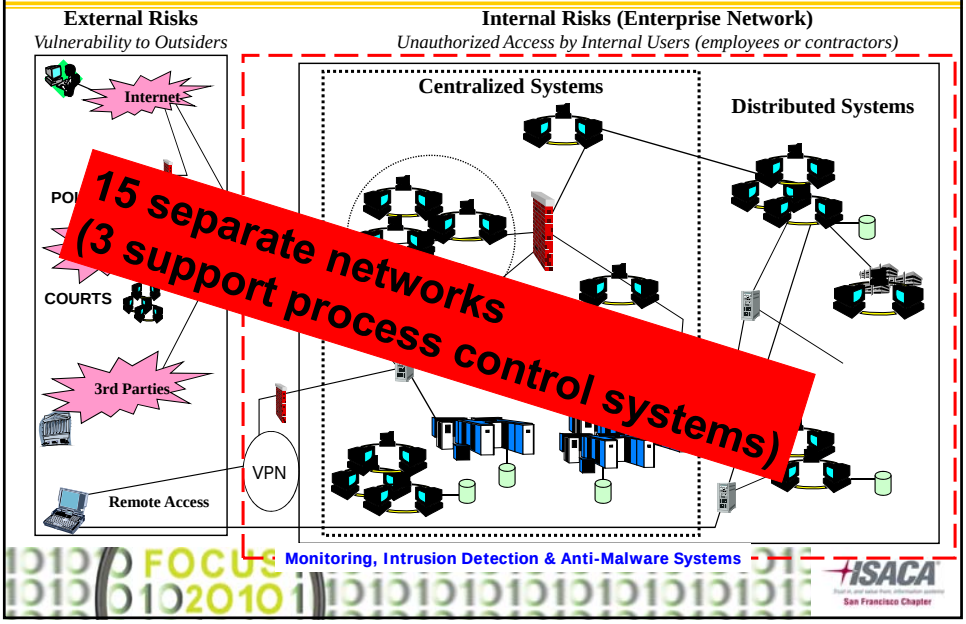
Business Services
- Development Services
- Phoenix Convention Center
- Community & Economic Development
- Downtown Development

Public Representation
- Mayor's Office
- Council Staff

FOCUS 2010

ISACA San Francisco Chapter

A Decentralized IT Infrastructure



FOCUS 2010

ISACA San Francisco Chapter

Initial City-wide IT Risk Assessment

- Teamed With *IT Audit Partner* (City Audit & KPMG)
  - Completed during 2005
  - Evaluated the City's overall IT risk profile
  - Identified and assessed IT risks and IT-related controls City-wide
- Risk Assessment Approach
  - Surveyed City Departments
  - Interviewed City Departments
  - Limited Validation / Follow-up / Research
  - Compiled application & system inventories
  - Prioritized risk areas

Initial City-wide IT Risk Assessment

- Evaluated Multiple Dimensions of Risk
  - Assessed Inherent, Control, and Residual Risk
- Results:
  - City-wide Risk Summary
    - Documented *Top 6 City-wide High Risk Areas*
      - *IT Governance* was the top risk reported
    - Documented *Top 12 Localized (i.e., departmental) Risk Areas*
      - Assigned a score of probability and magnitude for each dimension of risk (high, med, low)

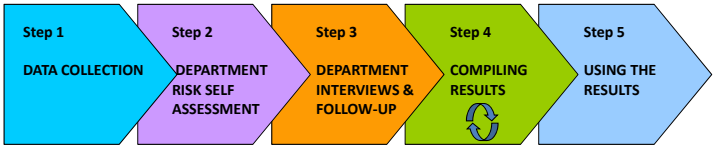
Initial City-wide IT Risk Assessment

– Departmental Risk Summary

– Prioritized System / Application Inventory
- Prioritized City-wide inventory of systems and applications

– Application Assessment
- ***Population:*** 467 systems / applications used throughout the City
- ***Critical Applications:*** 104 applications supporting critical operational and financial activities
- ***Sensitive Data:*** 159 applications process or store sensitive / confidential information
- ***Vendor Support:*** 290 systems / applications no longer supported
- ***Home-Grown Applications:*** 121 applications internally developed

Overview of Our Initial Approach



- 1 – Data Collection
  - ✓ Update Technology Environment Understanding
  - ✓ Update Application Inventory
- 2 – Facilitate Department Risk Self-Assessments
- 3 – Follow-up On Data Collection / Assessments
- 4 – Compile Results
- 5 – Using the Results

Our Goals for the Initial Assessment

- Obtain a current "population" (inventory) of applications
- Identify application risks by type:
  - Inherent
  - Residual
- Rank applications by criticality
- Understand the City-wide "Technology Universe"
- Create a risk-based multi-year IT audit plan

Data Collection
(Exercise #1)

Step 1
DATA COLLECTION

- Where would you start?
- What lists would you extract the data from?

FOCUS 2010 ISACA San Francisco Chapter

Data Collection

Step 1

DATA COLLECTION

- We started with…
  - City's Y2K list of applications
- We then…
  - Reviewed our prior audits
  - Brainstormed with auditors to identify applications they were aware of or had experienced
  - Obtained IT plan documents from City departments as well as the IT Department's Technology Master Plan

Department Self-Assessment

Step 2

DEPARTMENT SELF ASSESSMENT

- We sent each department:

A. List of applications from Data Collection

B. High-level department-wide IT control questions (tailored questionnaire)

Department Self-Assessment
Continued

Step 2

DEPARTMENT SELF ASSESSMENT

- For each application, we asked them to:
  - Apply risk estimates for each application (scale of 1-5)
  - Add any applications not included in our list
    - e.g. database type, server platform, support (internal or 3rd Party) etc.
  - Complete missing information (such as vendor name or note that the application is in-house developed/maintained)

Department Self-Assessment
Continued

Step 2

DEPARTMENT SELF ASSESSMENT

- Example of department application identified during Data Collection

Application Name	Platform	Application Description	Criticality 1-5	Origin Date	In House or Vendor Developed	In House or Vendor Maintained
SAP R/3 Financial Management System	Unix, IBM, NT-(Imaging), DB2	This system is an industry-leading system, used enterprise-wide at the City of Phoenix. The business process automated by the system include: time and labor tracking, accounts payable accounting, billing, accounts receivable accounting, asset accounting, general ledger, GAAP and budgetary financial reporting, funds (budget) management, purchasing, inventory management, cost accounting, CIP project accounting, and plant maintenance functionality (work management, preventative maintenance scheduling).	5	7/1/98	SAP, Finance	SAP, Finance

Department Self-Assessment
Continued

Step 2

DEPARTMENT SELF ASSESSMENT

- High-level department-wide IT control questions related to:
  - Department organization
  - Information systems environment
  - Security controls
    - Physical and logical
  - System development and maintenance
  - Business continuity and disaster recovery

Department Interviews

Step 3

DEPARTMENT INTERVIEWS

- After Departments completed their Self-Assessments, we met with them 1-on-1 to discuss:
  - Risk ranking for each department application
  - Completeness of application population
  - Applications with sensitive data
  - Overall department IT controls

Department Interviews
Continued

Step 3

DEPARTMENT INTERVIEWS

For **high-risk** applications, we discussed:

- Inherent Risk
  - The risk of an application/data without any controls
- Residual Risk
  - Estimated risk after considering existing controls

Department Interviews
Continued

Step 3

DEPARTMENT INTERVIEWS

- Which of the following applications do you think has the highest INHERENT RISK?
  - E-Commerce Electronic Payments to City
  - Court Management System
  - Underground Fuel Leak Detection System
  - Traffic Signals

FOCUS 2010 ISACA San Francisco Chapter

Department Interviews
Continued

Step 3

DEPARTMENT INTERVIEWS

- IT General Controls:
  - Access to Programs and Data
  - Change Management
  - Program Development
  - Computer Operations
  - BCM/DRP

Department Interviews
Continued

Step 3

DEPARTMENT INTERVIEWS

Interrogation	Situation
What controls do you have in place to ensure adequate network security?	If I am a hacker and I try to penetrate your network internally and/or externally, what controls do you have in place to prevent me from gaining access?
Do you have a plan in place in the event of a disaster?	What happens if a truck spills toxic chemical in front of your building entrance?
Why is Application A critical to your process?	If we remove Application A from the equation, so what? What is the impact?

Department Interviews
Continued

Step 3

DEPARTMENT INTERVIEWS

Interesting findings from these evaluations:

- First 10 minutes of the interview, we realized they had inadequate IT general controls.
- A high-risk application server was stored in the closet of the men's restroom.

Compiling Results

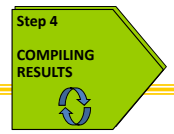
Step 4

COMPILING RESULTS

- Three primary outputs:
  - Application Risk Summary
  - Department Risk Summary
  - Citywide High-Risk Areas

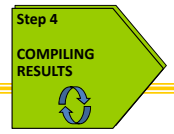
FOCUS 102010 ISACA San Francisco Chapter

Compiling Results (Applications)



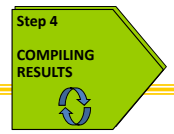
- Volume of Data
  - 25 departments
  - 467 applications
  - 2 risk categories
    - Inherent
    - Residual
- 5 Application Risk Types (see next slide)

Compiling Results (Applications)



- Application Risk Categories:
  - Data Sensitivity/Confidentiality
    - What is negative impact if information is public?
  - Data Integrity
    - What is the negative impact if the data is incomplete and/or inaccurate?
  - Data Availability
    - What is the negative impact if the data is unavailable?
  - Project
    - How often is the application changed, upgraded, patched, etc.?
  - Fraud
    - What damage can someone do from obtaining the information?

Compiling Results
(Applications)

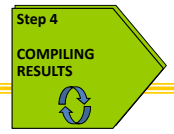


Those were the typical risk categories.
In addition to those on the previous slide,
what risk categories would you add?

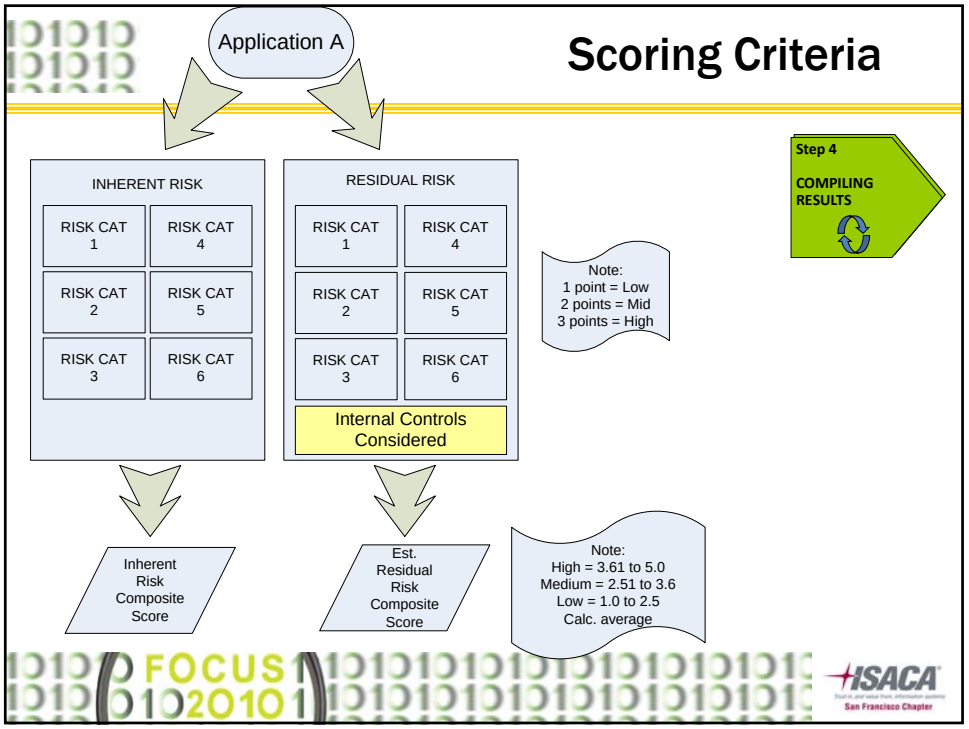
We had to add one (as a municipality):

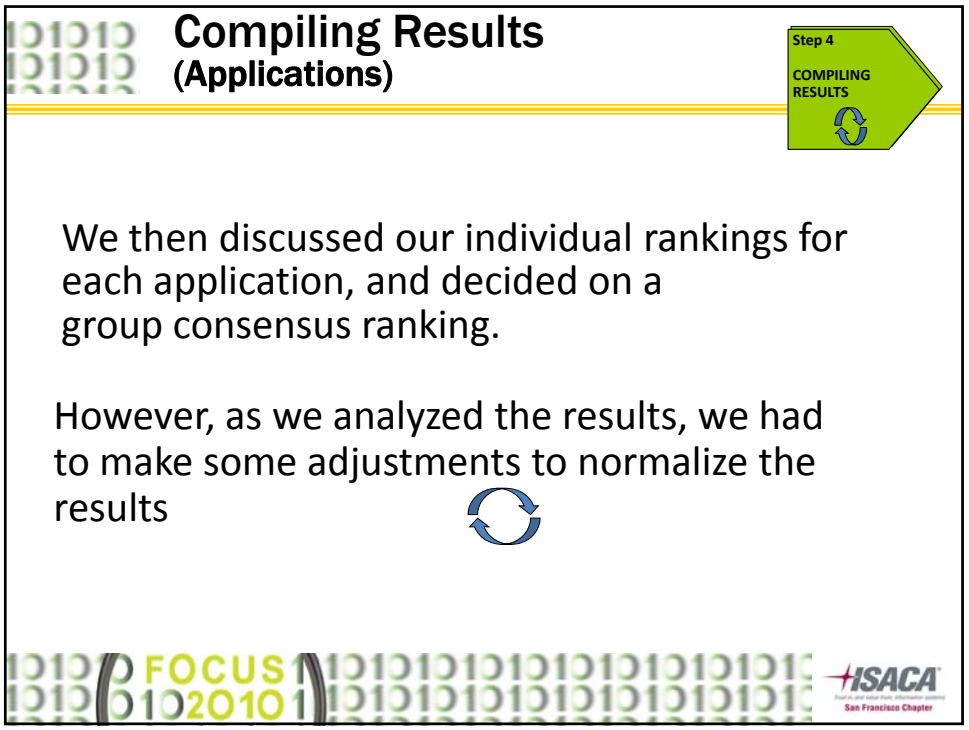
Public Safety

Compiling Results
(Applications)



- Each of us scored each application and each risk category without bias
  - Only using the information obtained from the interviews and questionnaires
  - Using both Inherent and Residual Risk
  - No substantive testing


Application A
Scoring Criteria
INHERENT RISK
RISK CAT 1
RISK CAT 4
RISK CAT 2
RISK CAT 5
RISK CAT 3
RISK CAT 6
RESIDUAL RISK
RISK CAT 1
RISK CAT 4
RISK CAT 2
RISK CAT 5
RISK CAT 3
RISK CAT 6
Internal Controls Considered
Step 4
COMPILING RESULTS
Note:
1 point = Low
2 points = Mid
3 points = High
Inherent Risk Composite Score
Est. Residual Risk Composite Score
Note:
High = 3.61 to 5.0
Medium = 2.51 to 3.6
Low = 1.0 to 2.5
Calc. average
FOCUS 2010
ISACA
San Francisco Chapter


Compiling Results
(Applications)
Step 4
COMPILING RESULTS
We then discussed our individual rankings for each application, and decided on a group consensus ranking.
However, as we analyzed the results, we had to make some adjustments to normalize the results
FOCUS 2010
ISACA
San Francisco Chapter

Compiling Results
(Applications)

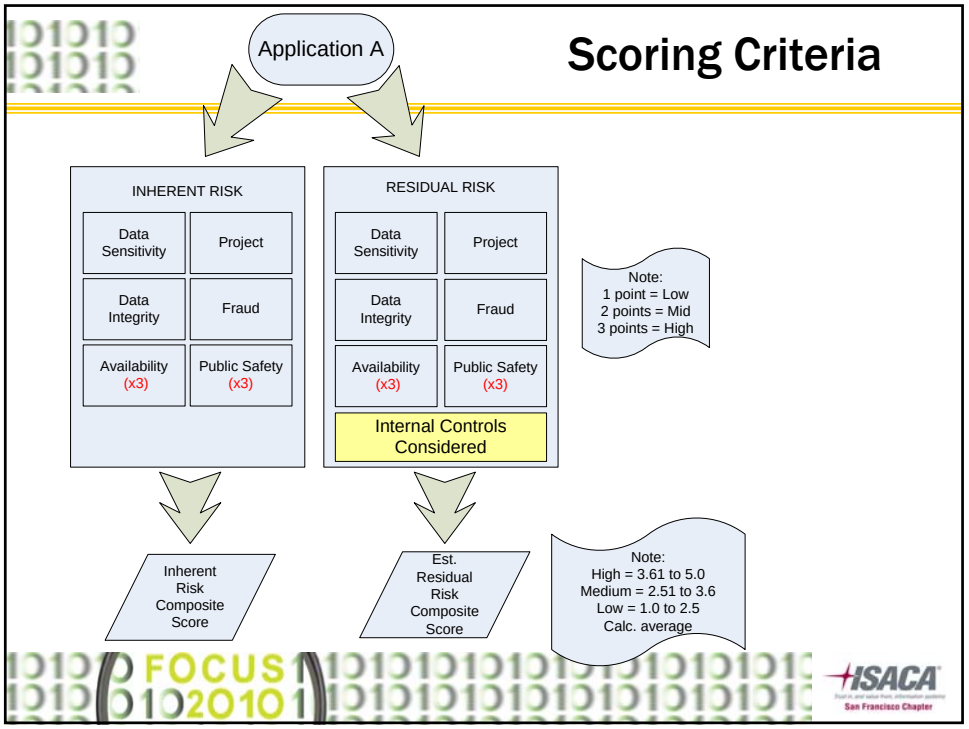
Step 4
COMPILING RESULTS

For example:

Initially, our 911 system was ranked as the 45th most critical application

It should be near #1

Thus, we adjusted the scoring criteria to more heavily weight the Public Safety and Data Availability Risk category



Compiling Results
(Applications)

Step 4
COMPILING RESULTS

	911 CAD System		SAP Financial System		Court Management System		Aviation Security Access System	
	Inherent	Residual	Inherent	Residual	Inherent	Residual	Inherent	Residual
Data Sensitivity	3	2	2	1	3	2	3	2
Data Integrity	3	2	3	2	3	2	2	1
Data Availability	3	2	3	2	2	1	3	2
Project	1	1	3	2	1	1	1	1
Fraud	1	1	3	2	1	1	1	1
Public Safety	3	2	1	1	3	2	3	2
Total	2.33	1.67	2.50	1.67	2.17	1.50	2.17	1.50
Weighted Total	4.33	3.00	3.83	2.67	3.83	2.50	4.17	2.83

Compiling Results
(Departments)

Step 4
COMPILING RESULTS

- Three primary outputs:
  - Application Risk Summary
  - Department Risk Summary
  - Citywide High Risk Areas

Compiling Results (Departments)

Step 4
COMPILING RESULTS

- We also compiled results and risk-ranked departments.

Highest Ranked Department	Lowest Ranked Department
• Highest average application inherent risk • High average application residual risk	• Lowest average application inherent risk • Low average application residual risk

Compiling Results (Departments)

Step 4
COMPILING RESULTS

- Which of the following 3 Departments do you think has the highest inherent risk?
  - Personnel
  - Water
  - Finance

Compiling Results (Departments)

Step 4
COMPILING RESULTS

- Which of the following 3 Departments has the highest inherent risk?
  - Personnel
  - **Water**
  - Finance

Due to constant availability requirements, data confidentiality, and public safety

Compiling Results (Departments)

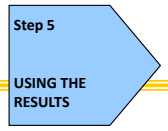
Step 4
COMPILING RESULTS

- Three primary outputs:
  - Application Risk Summary
  - Department Risk Summary
  - Enterprise-wide High Risk Areas

Compiling Results (Departments)

- We also identified some enterprise-wide risk factors such as:
  - IT Governance
  - Disaster Recovery / Business Continuity Planning
  - ITD Backup Power Source
  - Network
  - Vendor Support
  - Wireless

Using The Results



- Multi-Year IT Audit Plan
  - Department General IT Controls Reviews
  - Application Audits
  - Network Vulnerability Assessment
  - IT Governance and Policy Review
- Integration with current technology processes
  - Integrated with City's Oracle database (Technology Information System)
  - Integrated into the City-wide Technology Budget Planning process
- Ongoing / Annual update of data
  - Annual update (in process)

Some Lessons Learned

- Leverage existing data
- Each department had their own personality and during meetings we had to adjust to their focus
- Be prepared for anything

Surprises

- We performed the initial review right after Hurricane Katrina, so it was easy for people to identify risk
- Significant number of MS Excel and Access files
- City's election system is critical to the organization, but didn't fit into many of the risks identified

Surprises

- Sensitive/Confidential data is more than just SSN, Credit Cards, HIPAA:
  - Police and Judge personal information
  - Infrastructure information (e.g., utilities)
  - Others (e.g., Hazmat, Aviation security, etc.)
- Process control systems (e.g., Convention Center HVAC, Water Treatment System)

Components of an Effective
Ongoing City-wide IT Risk Assessment Process

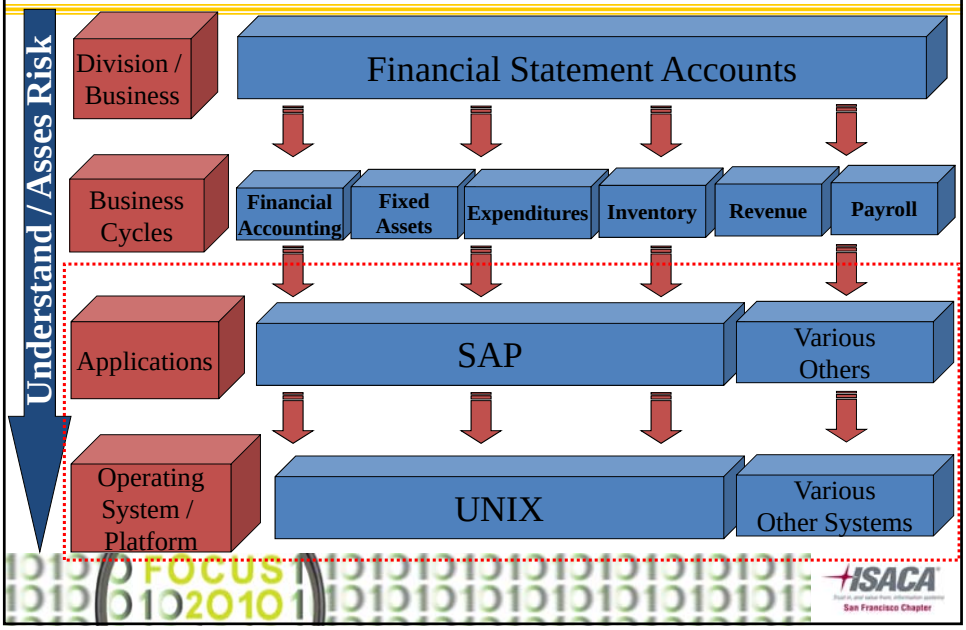
IT Risk Assessment @ City Today

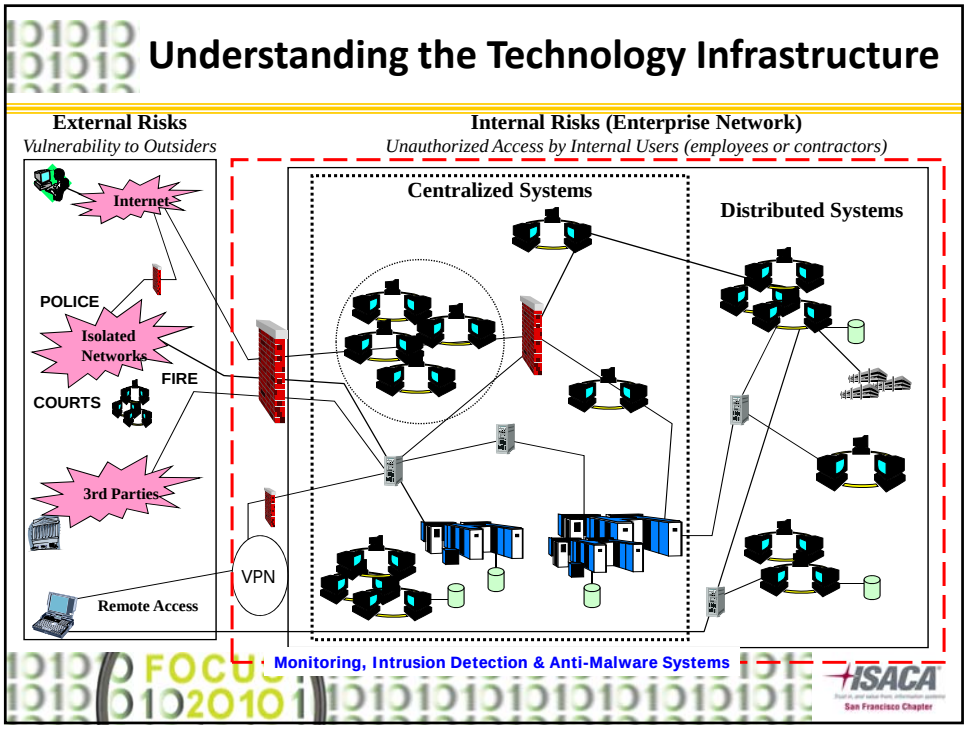
- Understand Technology Universe
- Define Technology Audit Universe
- Distributed Infrastructure Risk Assessments
- Application Risk Assessments
- Other
  - Business Cycle Analysis
  - System Implementation / Replacement / Upgrades
  - City Initiatives Impacting Technology

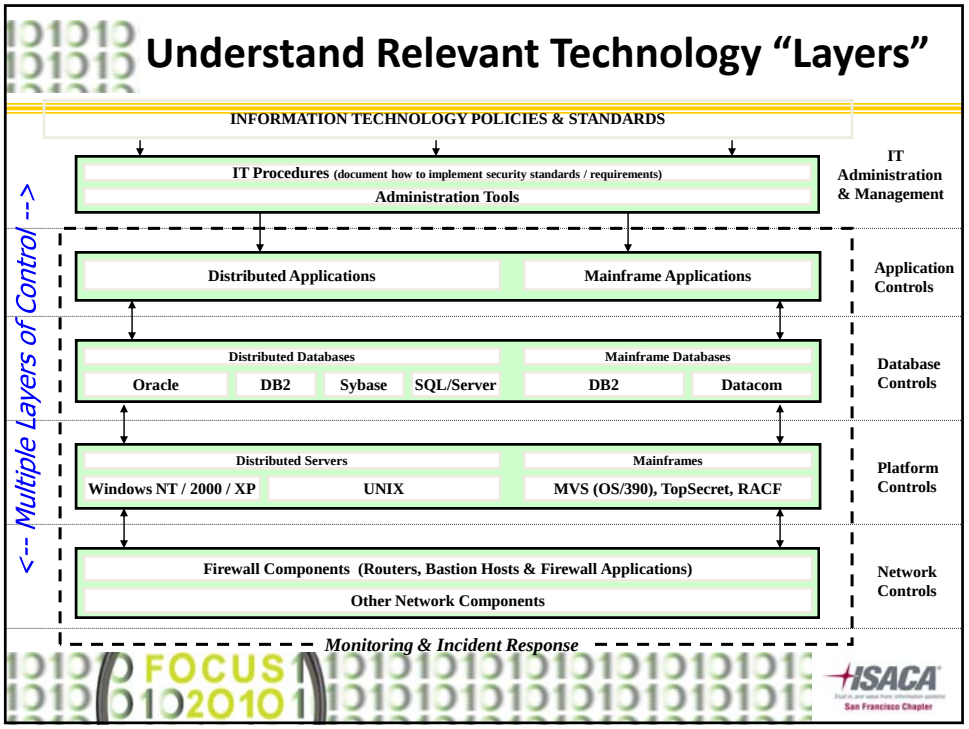
Understand *Technology Universe*

- Technology Infrastructure
- IT Human Resources
- IT Management & Support Structure
- IT Strategic Plan /Budget

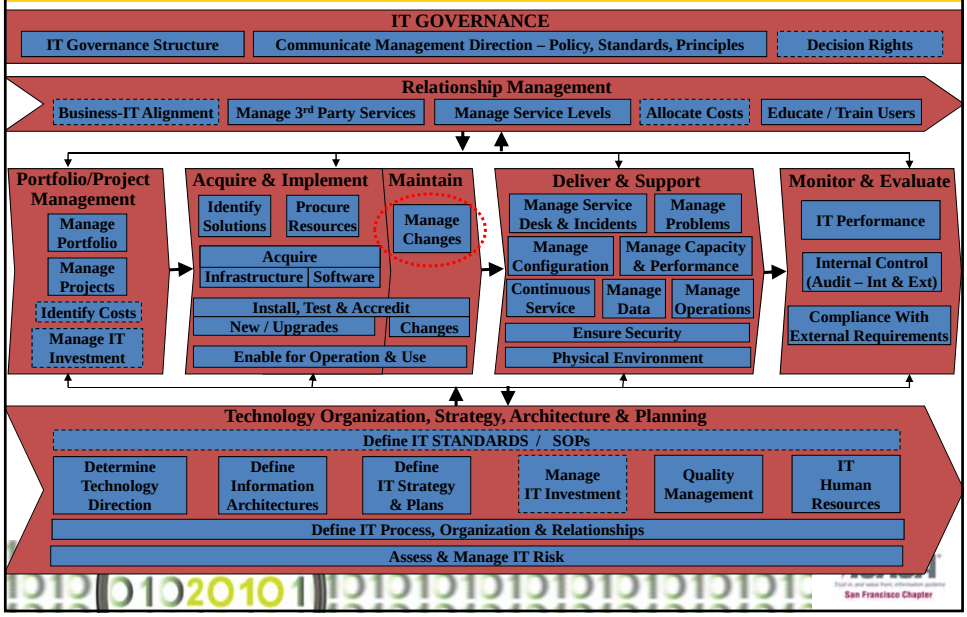
Technology Infrastructure
Linkage to Business



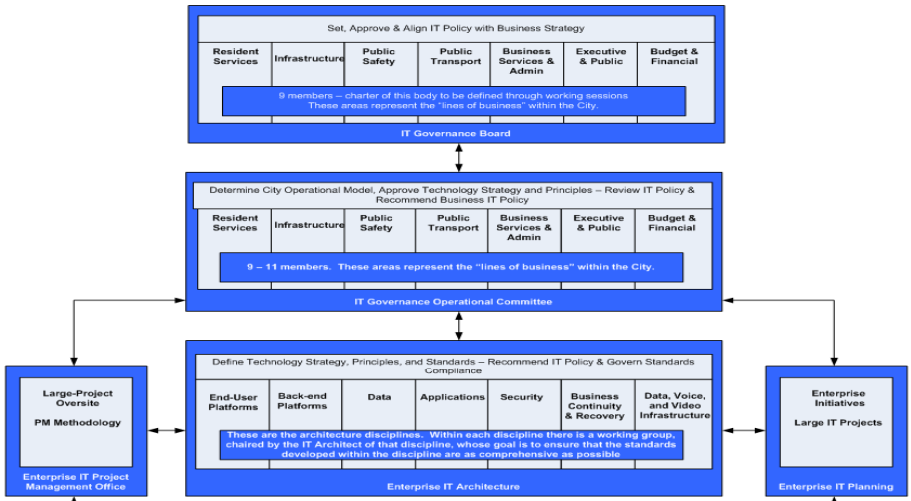

Understanding the Technology Infrastructure
External Risks
Vulnerability to Outsiders
Internal Risks (Enterprise Network)
Unauthorized Access by Internal Users (employees or contractors)
Internet
POLICE
Isolated Networks
FIRE
COURTS
3rd Parties
Remote Access
VPN
Centralized Systems
Distributed Systems
Monitoring, Intrusion Detection & Anti-Malware Systems
FOCUS 2010
ISACA
San Francisco Chapter


Understand Relevant Technology "Layers"
INFORMATION TECHNOLOGY POLICIES & STANDARDS
IT Procedures (document how to implement security standards / requirements)
Administration Tools
IT Administration & Management
<-- Multiple Layers of Control -->
Distributed Applications
Mainframe Applications
Application Controls
Distributed Databases
Oracle
DB2
Sybase
SQL/Server
Mainframe Databases
DB2
Datacom
Database Controls
Distributed Servers
Windows NT / 2000 / XP
UNIX
Mainframes
MVS (OS/390), TopSecret, RACF
Platform Controls
Firewall Components (Routers, Bastion Hosts & Firewall Applications)
Other Network Components
Network Controls
Monitoring & Incident Response
FOCUS 2010
ISACA
San Francisco Chapter

Understanding the *Process Universe*



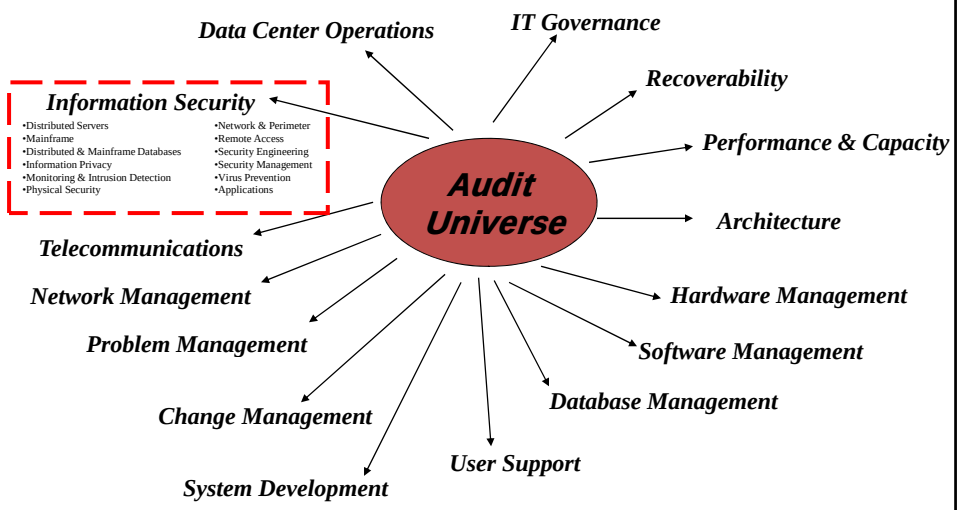
Understanding the IT Governance Structure



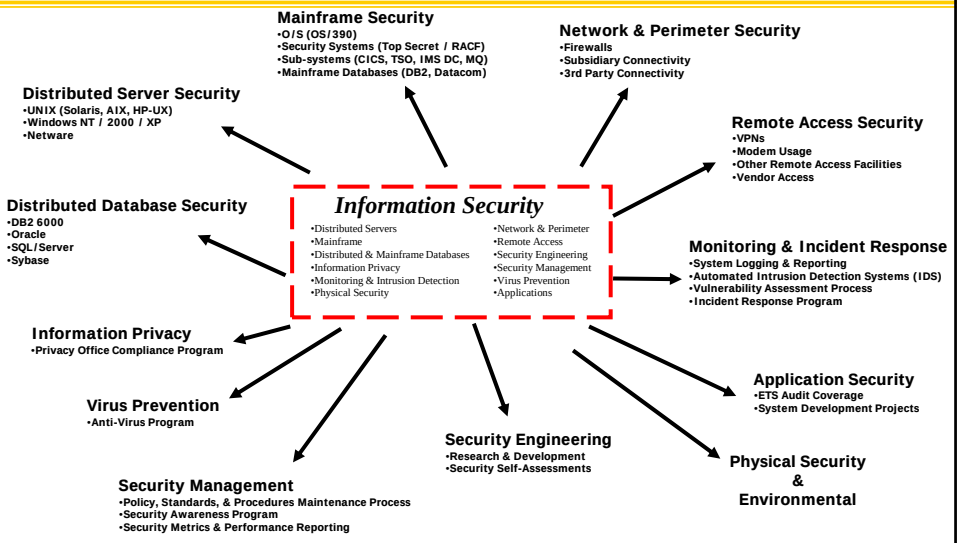
Understand *Technology AUDIT Universe*

- IT Platforms
- Applications
- Data / Computer Centers
- Information / Data (Classification)

Defining the *Technology Audit Universe*



Security Audit Universe

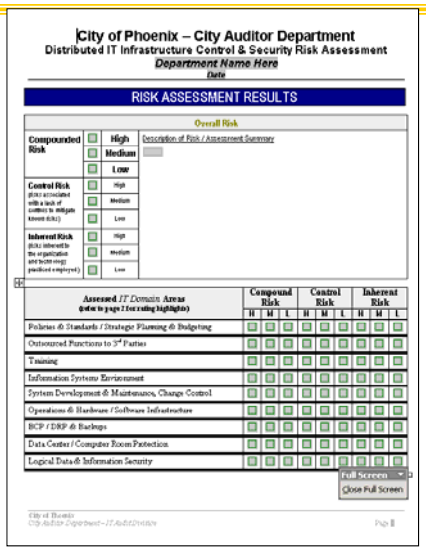


Distributed IT Infrastructure

Security & Control Risk Assessments

Focus

IT General Controls


City of Phoenix – City Auditor Department

Distributed IT Infrastructure Control & Security Risk Assessment

Department Name Here

Date

RISK ASSESSMENT RESULTS

Overall Risk

Compounded Risk	High / Medium / Low	Description of Risk / Assessment Summary
Control Risk	High / Medium / Low	
Inherent Risk	High / Medium / Low	

Assessed *IT Domain* Areas (refer to page 2 for scoring highlights)	Compound Risk H M L	Control Risk H M L	Inherent Risk H M L
Policies & Standards / Strategic Planning & Budgeting			
Outsourced Functions to 3rd Parties			
Training			
Information Systems Environment			
System Development & Maintenance, Change Control			
Operations & Hardware / Software Infrastructure			
BCP / DRP & Backups			
Data Center / Computer Room Protection			
Logical Data & Information Security			

Full Screen

Close Full Screen

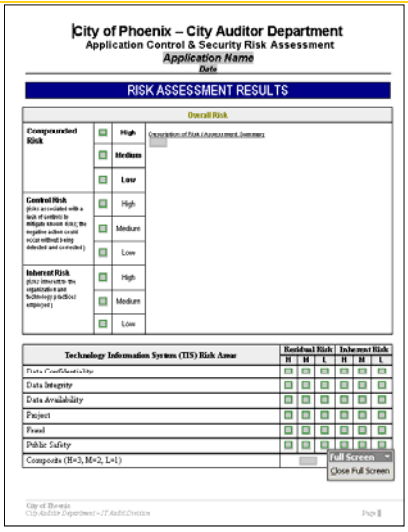
City of Phoenix
City Auditor Department – IT Audit Division

Page 1

Applications
Security & Control Risk Assessments

Focus

Application Controls


City of Phoenix – City Auditor Department
Application Control & Security Risk Assessment
Application Name
Date
RISK ASSESSMENT RESULTS
Overall Risk
Compounded Risk
Control Risk
Inherent Risk
High
Medium
Low
Technology Information System (IIS) Risk Area
Residual Risk
Inherent Risk
Data Integrity
Data Availability
Project
Fraud
Public Safety
Composite (H=3, M=2, L=1)
Full Screen
Close Full Screen

FOCUS 2010

ISACA San Francisco Chapter

Technology Specific
Security & Control Risk Assessments

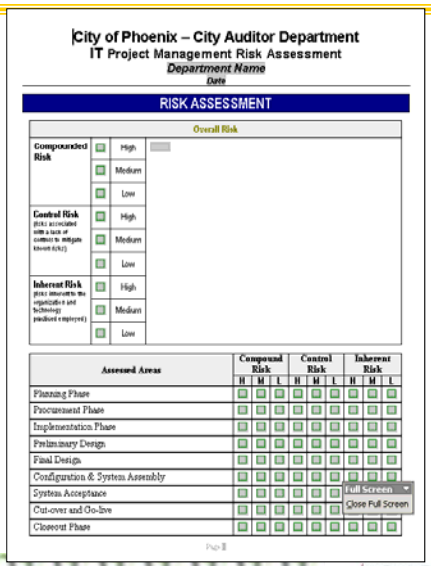
Examples:

-OS Config & Patch Mgt

-IT Project Management

-Privacy

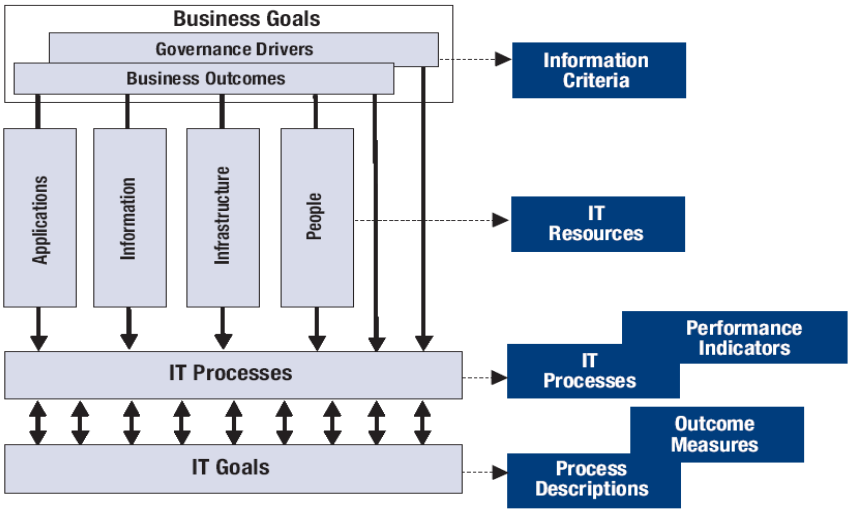
-Information Security


City of Phoenix – City Auditor Department
IT Project Management Risk Assessment
Department Name
Date
RISK ASSESSMENT
Overall Risk
Compounded Risk
Control Risk
Inherent Risk
High
Medium
Low
Assessed Areas
Compound Risk
Control Risk
Inherent Risk
Planning Phase
Procurement Phase
Implementation Phase
Preliminary Design
Final Design
Configuration & System Assembly
System Acceptance
Cut-over and Go-live
Closeout Phase
Full Screen
Close Full Screen

FOCUS 2010

ISACA San Francisco Chapter

IT Governance (Business Goals Drive IT Goals)
Business Cycle Analysis & Risk Assessment

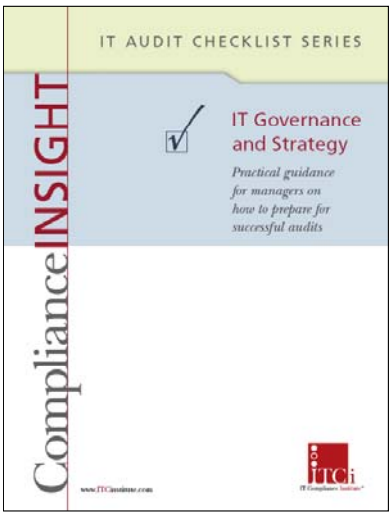


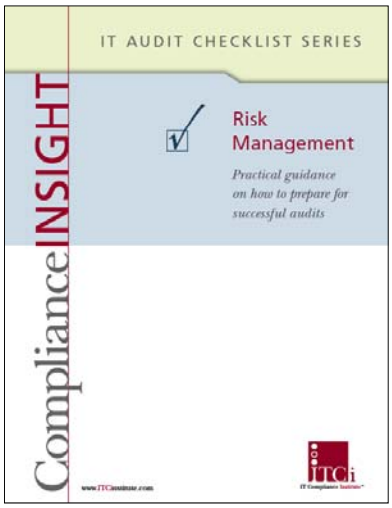
IT Governance (Business Goals Drive IT Goals)
Business Cycle Analysis & Risk Assessment

DIVISION [Start typing here]
OPERATING AREA [Start typing here]

#	KEY PROCESS	RISK/ POTENTIAL ERROR	POSSIBLE NEGATIVE RESULTS	EXISTING CONTROL(S) TO PREVENT OR DETECT RISK	CLIENT'S ASSESSMENT OF RISK CONSEQUENCE (10 = significant 1 = insignificant)	CLIENT'S ASSESSMENT OF CONTROL EFFECTIVENESS (10 = ineffective 1 = effective)	CLIENT'S NET RISK & CONTROL VALUATION (100 = high to low = 1)	AUDITOR'S EVALUATION OF RISK (High / Medium / Low)	AUDITOR'S EVALUATION OF PROBABLE CONTROL EFFECTIVENESS (Highly / Moderate / Slightly / Ineffective / Not Sure)	AUDIT FOCAL AREA (yes / no)	AUDIT FOCAL AREA AUDIT OBJECTIVES (control tests / control development / other)	AUDIT PRIORITY (High Priority / Medium Priority / Low Priority)
	(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)	(I)	(J)	(K)	(L)
1												

Resources
IT Compliance Institute





FOCUS 2010

ISACA San Francisco Chapter

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

Conducting Enterprise- Wide IT Risk Assessments

Questions?

Thank You!

FOCUS 2010
Critical Skills ○ Risk ○ Your Network

For More Information

Lance Turcato, CGEIT, CISA, CISM, CPA, CITP
Deputy City Auditor
City of Phoenix
City Auditor Department – IT Audit Division
lance.turcato@phoenix.gov