G11 - Convergence of IT Security & Compliance

Stephen Spalding

September 21, 2009 – September 23, 2009

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

The Convergence of Regulatory Environments, Risk Management, and IT Audit

On Track Consulting

Stephen Spalding, Partner

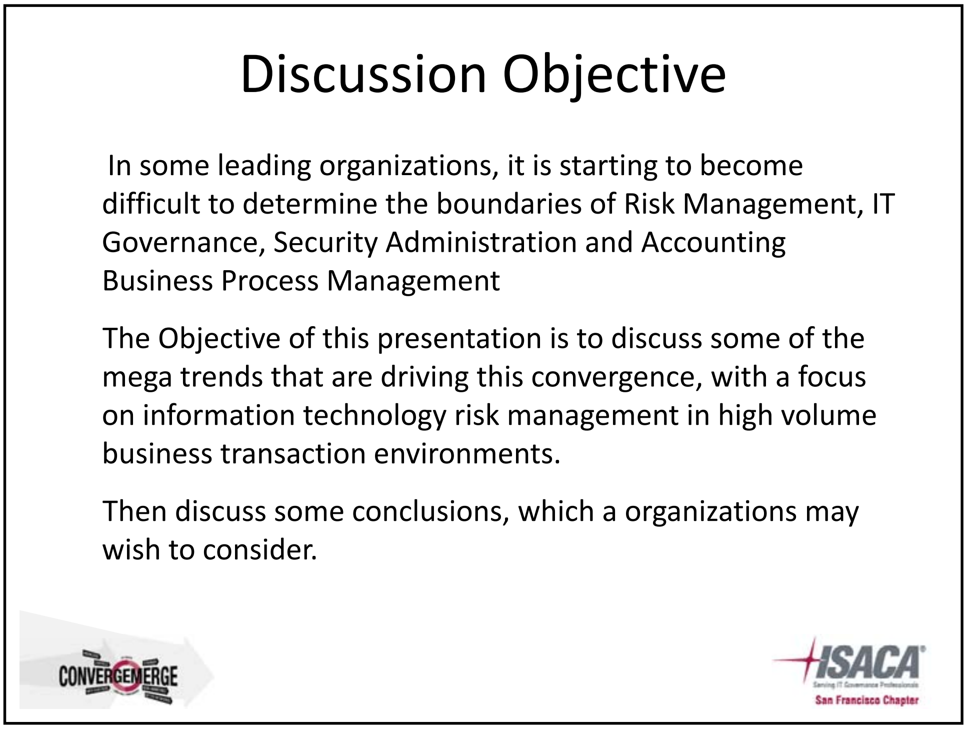
September 21, 2009 – September 23, 2009

ISACA
Serving IT Governance Professionals
San Francisco Chapter

Discussion Topics

- Discussion Objectives
- Convergence
- Mega Trends
- Risk
- Business: Risk Models
- IT: Risk Models
- Organizational Requirements
- Security Administration
- IT Application Governance
- Conclusions

ISACA
Serving IT Governance Professionals
San Francisco Chapter

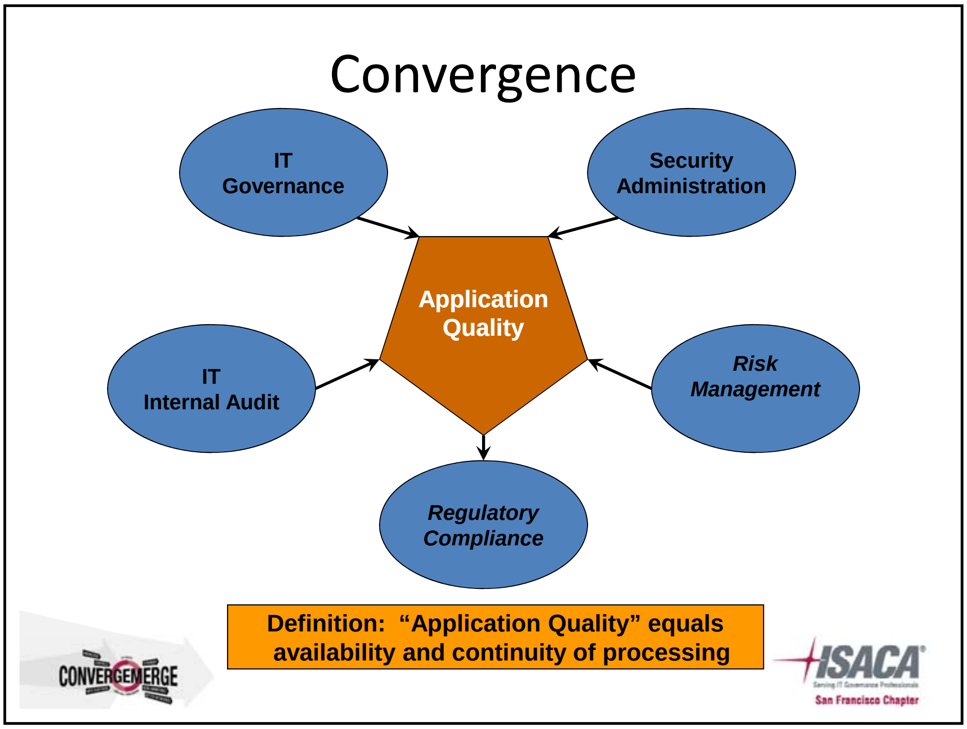


Discussion Objective

In some leading organizations, it is starting to become difficult to determine the boundaries of Risk Management, IT Governance, Security Administration and Accounting Business Process Management

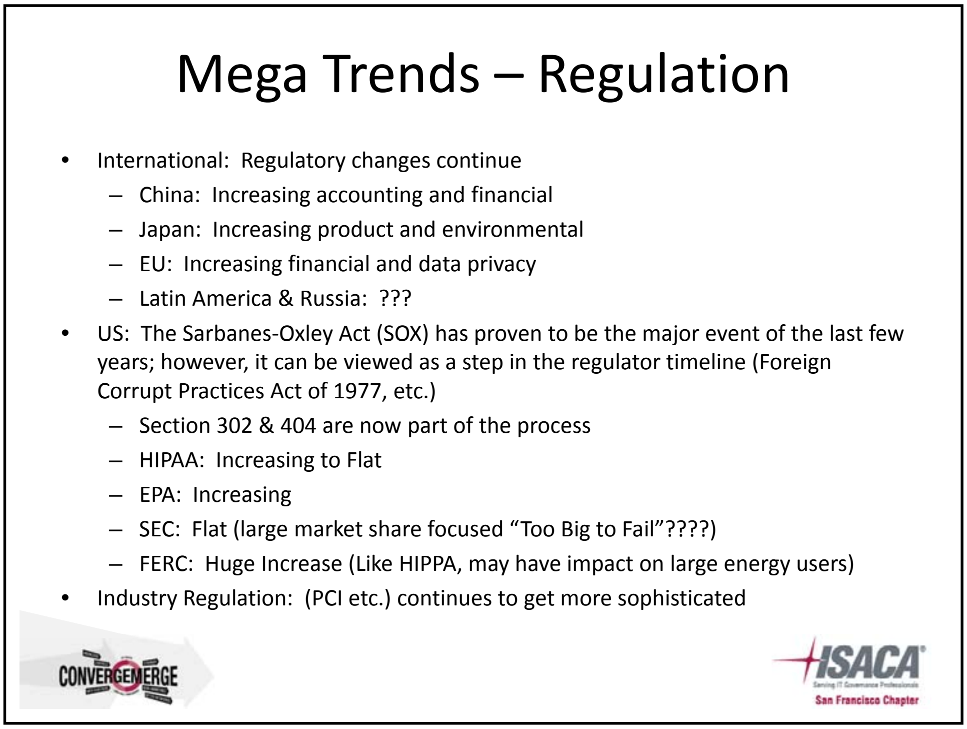
The Objective of this presentation is to discuss some of the mega trends that are driving this convergence, with a focus on information technology risk management in high volume business transaction environments.

Then discuss some conclusions, which a organizations may wish to consider.



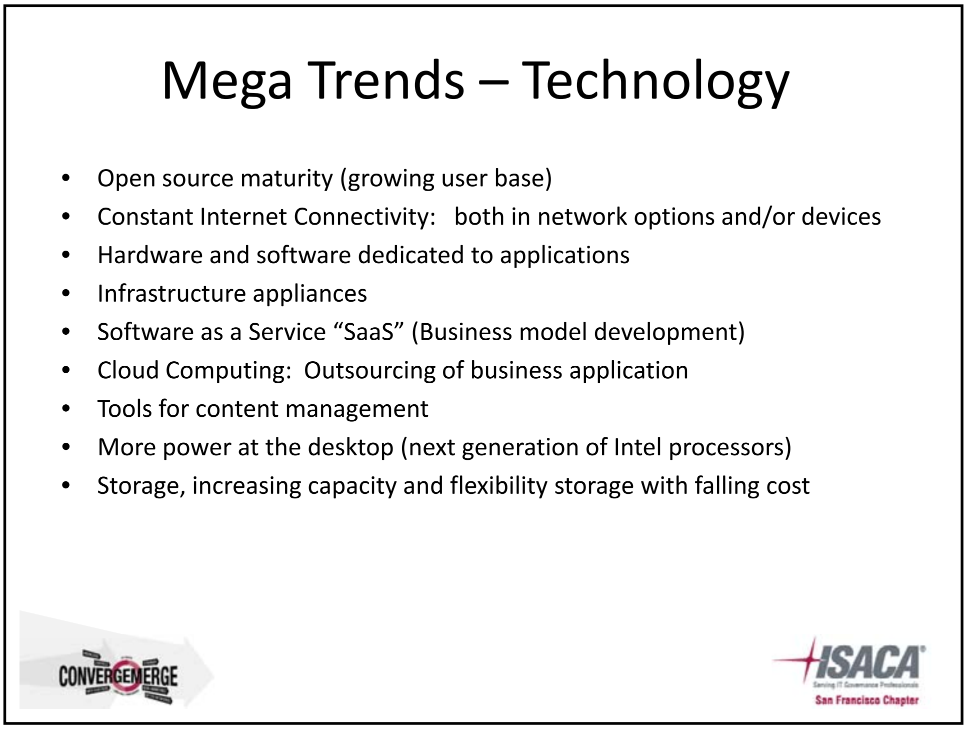
Convergence

Definition: “Application Quality” equals availability and continuity of processing



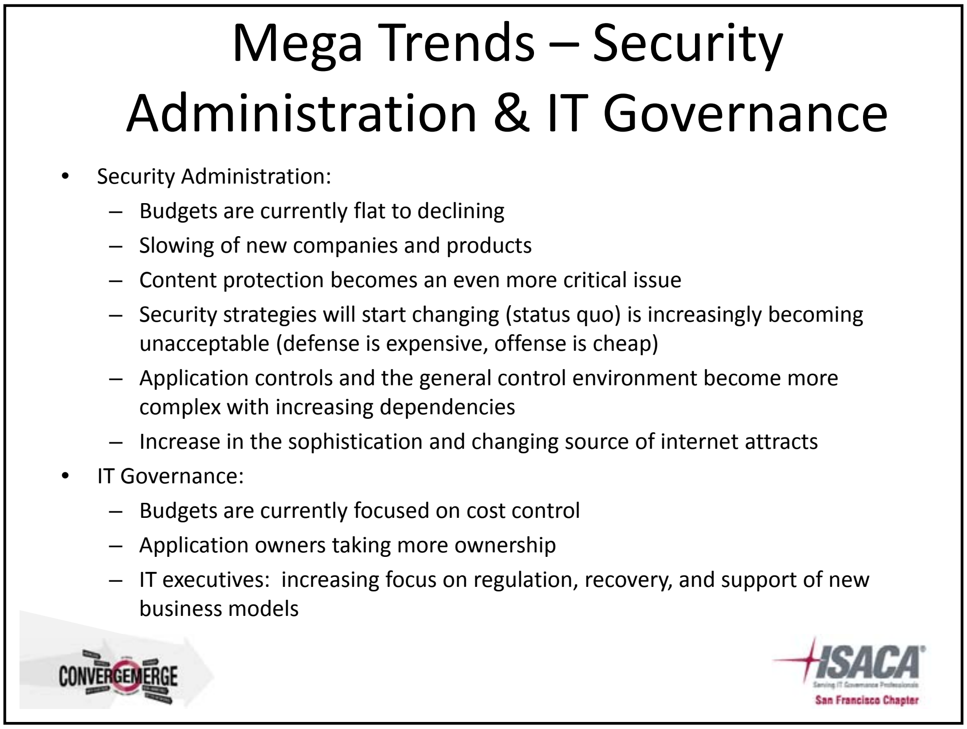
Mega Trends – Regulation

- International: Regulatory changes continue
  - China: Increasing accounting and financial
  - Japan: Increasing product and environmental
  - EU: Increasing financial and data privacy
  - Latin America & Russia: ???
- US: The Sarbanes-Oxley Act (SOX) has proven to be the major event of the last few years; however, it can be viewed as a step in the regulator timeline (Foreign Corrupt Practices Act of 1977, etc.)
  - Section 302 & 404 are now part of the process
  - HIPAA: Increasing to Flat
  - EPA: Increasing
  - SEC: Flat (large market share focused “Too Big to Fail”????)
  - FERC: Huge Increase (Like HIPPA, may have impact on large energy users)
- Industry Regulation: (PCI etc.) continues to get more sophisticated



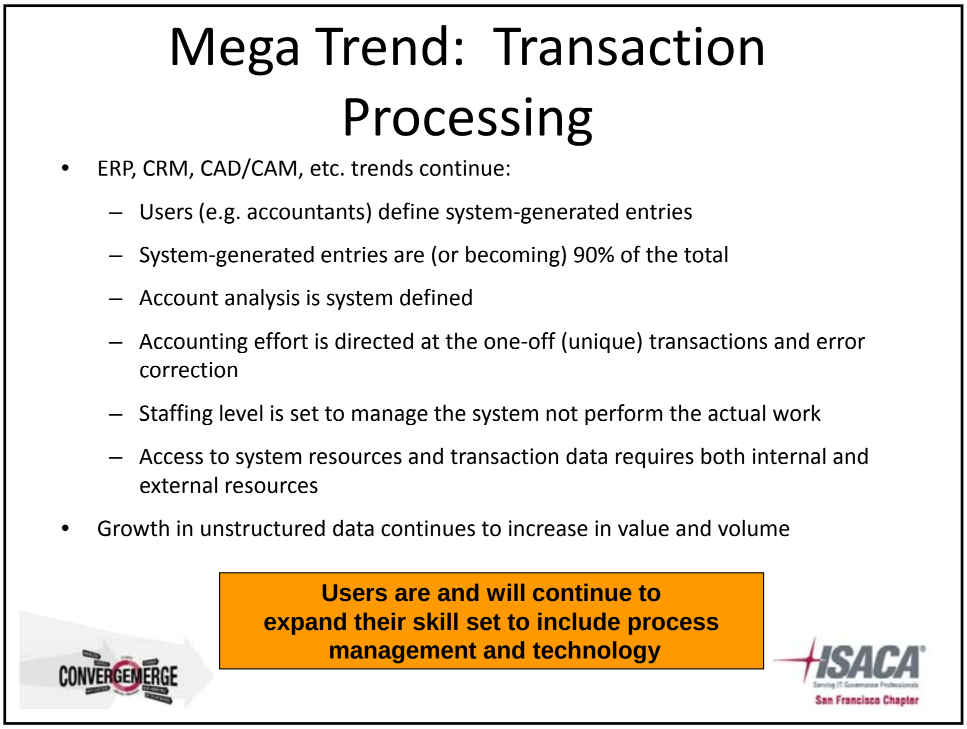
Mega Trends – Technology

- Open source maturity (growing user base)
- Constant Internet Connectivity: both in network options and/or devices
- Hardware and software dedicated to applications
- Infrastructure appliances
- Software as a Service “SaaS” (Business model development)
- Cloud Computing: Outsourcing of business application
- Tools for content management
- More power at the desktop (next generation of Intel processors)
- Storage, increasing capacity and flexibility storage with falling cost



Mega Trends – Security Administration & IT Governance

- Security Administration:
  - Budgets are currently flat to declining
  - Slowing of new companies and products
  - Content protection becomes an even more critical issue
  - Security strategies will start changing (status quo) is increasingly becoming unacceptable (defense is expensive, offense is cheap)
  - Application controls and the general control environment become more complex with increasing dependencies
  - Increase in the sophistication and changing source of internet attracts
- IT Governance:
  - Budgets are currently focused on cost control
  - Application owners taking more ownership
  - IT executives: increasing focus on regulation, recovery, and support of new business models



Mega Trend: Transaction Processing

- ERP, CRM, CAD/CAM, etc. trends continue:
  - Users (e.g. accountants) define system-generated entries
  - System-generated entries are (or becoming) 90% of the total
  - Account analysis is system defined
  - Accounting effort is directed at the one-off (unique) transactions and error correction
  - Staffing level is set to manage the system not perform the actual work
  - Access to system resources and transaction data requires both internal and external resources
- Growth in unstructured data continues to increase in value and volume

Users are and will continue to expand their skill set to include process management and technology

Trends: Organizational Impact

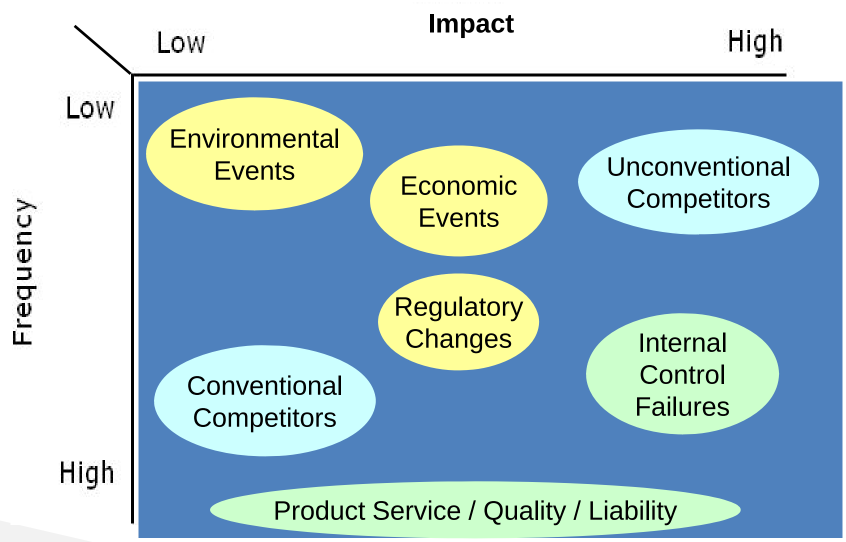
- Increasing transaction volumes
  - Mobile and dispersed workforce
  - Globally dispersed organizations
  - Globally expanding markets
- Diversifying base of technology
  - Increasing footprint of open source
  - Expanded channels of access, (mobile)
  - Increasing complexity of solutions and technologies
- Expanding and complex global regulatory environment
  - Increasing regulatory requirements for tighter demonstrable and documented controls
  - Increasing complexity of regulatory reporting
  - Constantly changing regulatory landscape
  - Application Portfolio not designed to support high regulatory change

These trends point to a high volume transaction based business with diversity in supporting technology

Risk

- Current Failures:
  - Most risk models and management process didn't see the TRAIN!
  - Budgets, Business Plans and product portfolio's were build on more of the same
- Major Rethink:
  - Short term
    - "Get Liquid ASAP"
    - Survival first, opportunity second
  - Longer term
    - Risk Management "How & Who?"
    - Risk Management Business Process?
      - Global view is a given
      - Need for change is understood
- University Programs

Business: Risk Model



Impact

Low

High

Frequency

Low

High

Environmental Events

Economic Events

Unconventional Competitors

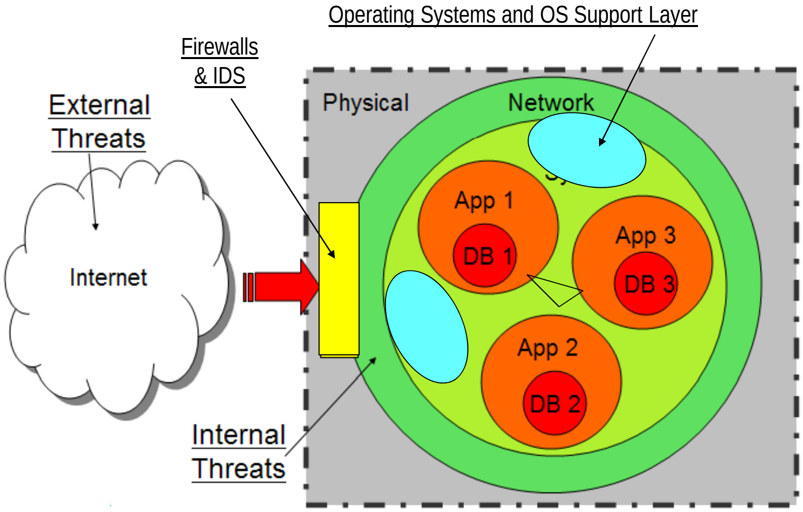
Regulatory Changes

Internal Control Failures

Conventional Competitors

Product Service / Quality / Liability

Technology Threats



Operating Systems and OS Support Layer

Firewalls & IDS

External Threats

Internet

Physical

Network

App 1

DB 1

App 3

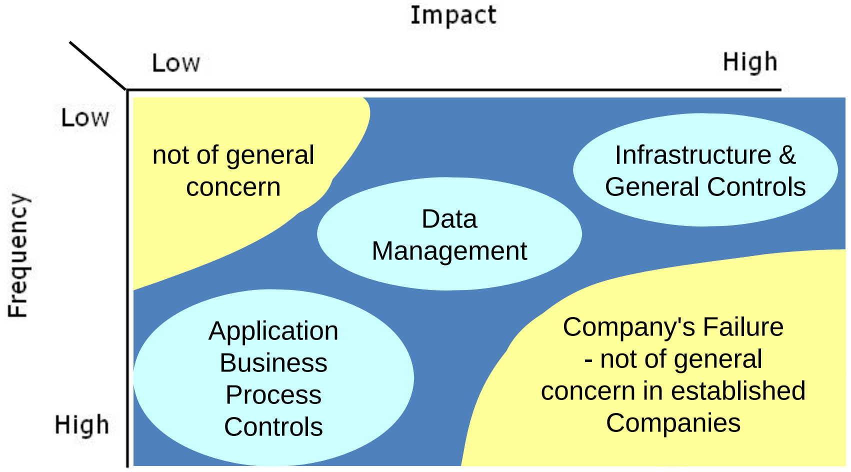
DB 3

App 2

DB 2

Internal Threats

IT: Risk Model



Impact

Low

High

Frequency

Low

High

not of general concern

Infrastructure & General Controls

Data Management

Application Business Process Controls

Company's Failure - not of general concern in established Companies

Organizational Requirements

Given these trends and risks, *“What are the key focal points for businesses with high volume transactions?”*

- Application Portfolio Quality
  - Availability
  - Continuity of Processing
- Effective Applications
  - Application Architecture
  - Application Deployment
- Regulator Compliance
  - Network and security administration
  - Application change control

Application and business processing quality is the key to a successful high volume transaction processing

Security Administration

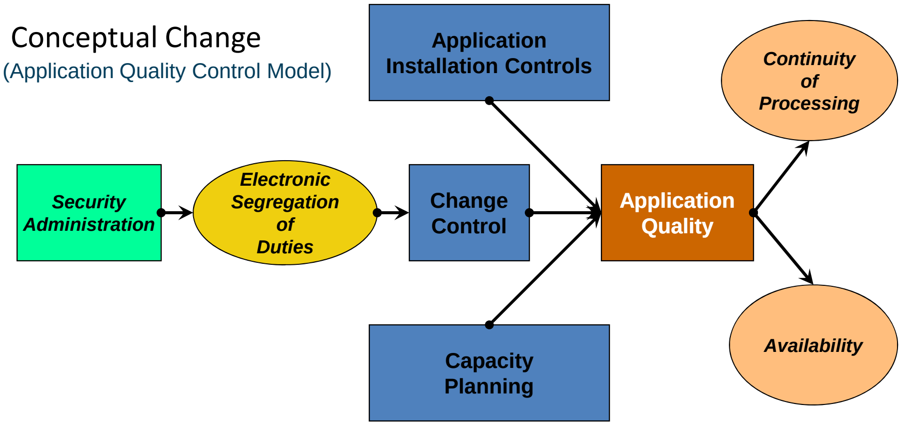
- Electronic Assets that require protection are expanding rapidly
- Regulator changes are increasing the cost and the risk of nonperformance
- Non-structured data is a huge problem
- Technology growth in devices and storage are adding to the complexity of the problem
- Data and processing complexity require increasing business processing expertise
- Current strategies are letting organizations down
  - The current bad guys don’t let you know that you have/are being hit
  - The current threats are well funded and organized (cipher crime pays)

The security administration role of “keeping the bad guys out” needs to change to “helping manage business applications”

IT Application Governance

Conceptual Change

(Application Quality Control Model)



Security Administration

Electronic Segregation of Duties

Change Control

Application Installation Controls

Capacity Planning

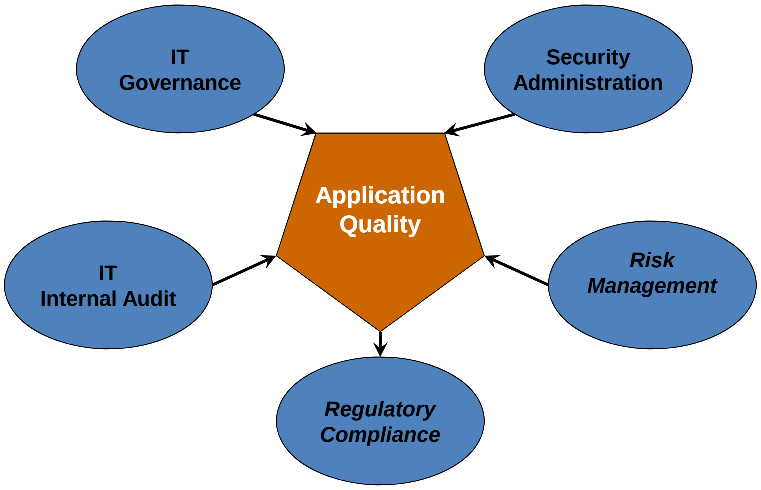
Application Quality

Continuity of Processing

Availability

Application Quality depends on the diligent exercise of Change Control

Convergence



IT Governance

Security Administration

Application Quality

IT Internal Audit

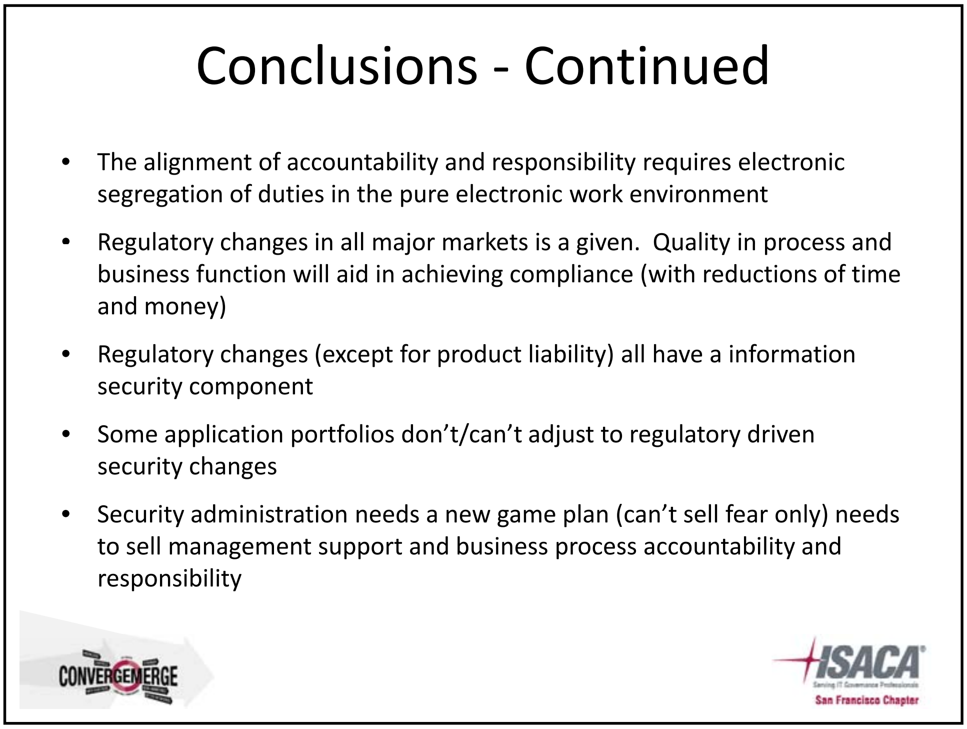
Risk Management

Regulatory Compliance

External trends that drive change
Require a focus on internal processes/ controls and application quality

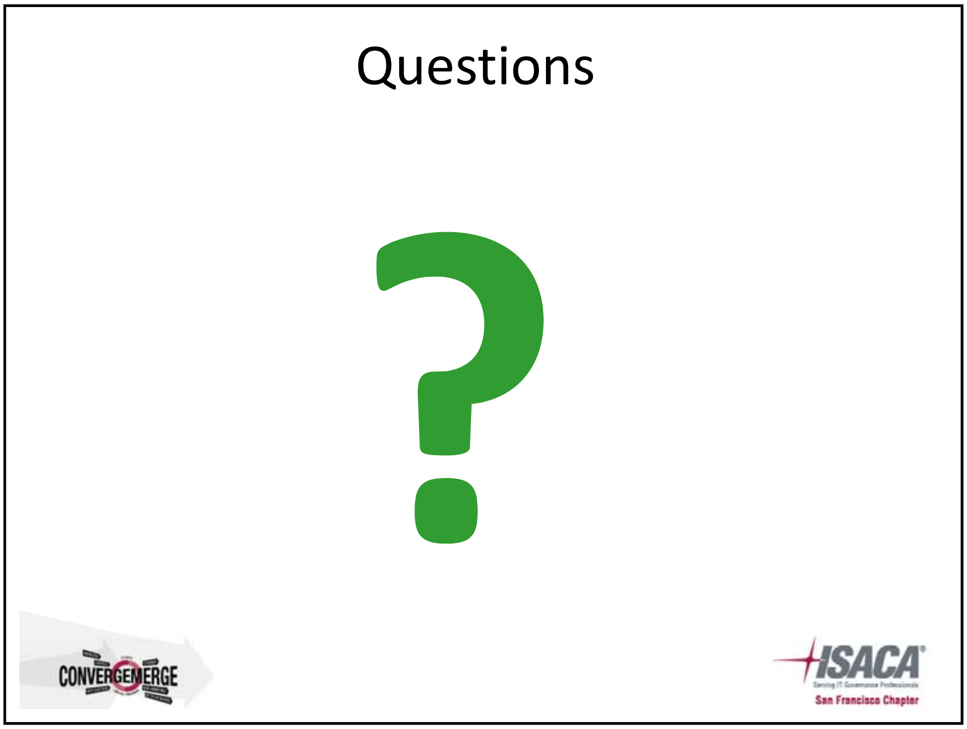
Conclusions

- Convergence of knowledge and skills requires increased organizational discipline and possible organizational adjustments
- As the ratio of transactions to employees continues to increase, the employees’ skill set and knowledge base (IT, accounting, application management) becomes mission critical
- Given the staffing to transaction ratio and that staff is organized to manage the application portfolio, timely recoverability is critical
- As transaction volumes grow, organizations place increasing reliance on the quality of their application portfolio. Measuring quality and setting goals should be considered
- Electronic segregation of duties and personnel management controls are the only real controls



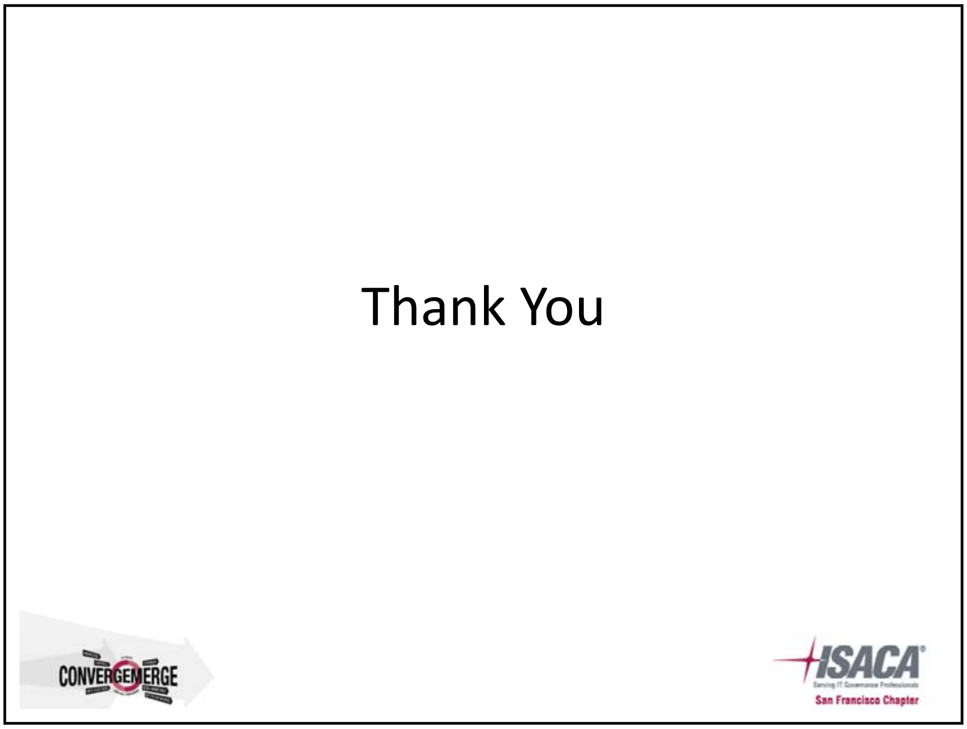
Conclusions - Continued

- The alignment of accountability and responsibility requires electronic segregation of duties in the pure electronic work environment
- Regulatory changes in all major markets is a given. Quality in process and business function will aid in achieving compliance (with reductions of time and money)
- Regulatory changes (except for product liability) all have a information security component
- Some application portfolios don't/can't adjust to regulatory driven security changes
- Security administration needs a new game plan (can't sell fear only) needs to sell management support and business process accountability and responsibility



Questions

?



Thank You