ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Convergence of Information Security & Compliance

September 22, 2008
Stephen Spalding, Partner
get2volume
sspalding@get2volume.com

Agenda

- Discussion Objectives
- Trends
- Security Administration
  - Risk Discussion
  - Risk Models
  - Risk Topics
- Risk Topics
- Transactional Risk
- IT Governance
- Organizational Impact
- Conclusions

Discussion Objective

In some leading organizations, it is starting to become difficult to determine the boundaries of Information Security, Risk Management and other organizational groups.

The Objective of this presentation is to discuss some of the key aspects of information security/organizational risk, with a focus on high volume business transaction environments.

Then draw some conclusions which some organizations may wish to consider.

Trends – Regulation Current Status

- Regulatory changes continue to advance in all major markets
- The Sarbanes-Oxley Act (SOX) has proven to be the major event of the last few years in the US; however, it can be viewed as a step in the regulator timeline (Foreign Corrupt Practices Act of 1977, HIPPA, GLBA etc.)
    - Section 302 is now part of the process
    - Section 404 is completed (or as complete as it well ever be)
        - Concerns over the impact are building among the SEC, business leaders, and other regulators
        - Most organizations are now in maintenance mode
    - Serious discussions at the SEC about changes seem to be under discussion (little change in current year given US elections).
- Foreign market regulator actions have increasing impact on a mounting number of large international organizations
- Regulatory risk is getting more attention in Information Security and Enterprise Risk Management groups

Trends – Technology Current Status

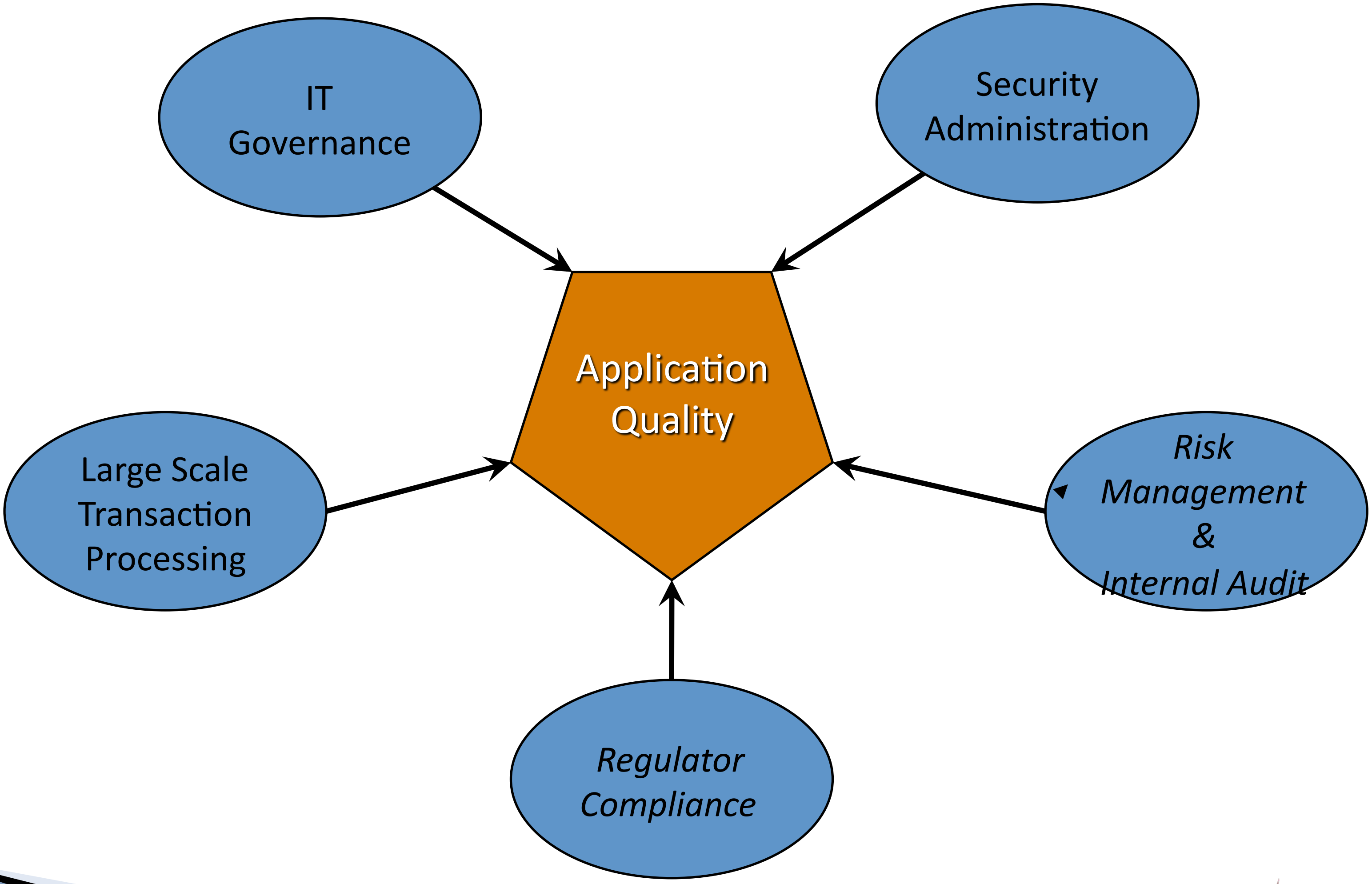
- Open source maturity (growing user base)
- Connectivity both in network options and/or devices expanding
- Tools for content management
- More power at the desktop
  - Hardware processing performance
  - New software tools (search, security, connectivity, etc.)
- Early stages of next generation of ubiquitous device
- Increasing capacity, flexible storage devices and falling cost
- Unstructured data continues to play a bigger role
- "Software as a Service" expands
- Outsourcing of business (applications) functions continue

Trends – Globalization Status

- Increasing wealth to new economies (e.g., China, India) - some members of the G8 become less important
- Increasing standards in communication continue to support global economic activity
- Outsourcing continues to migrate to lower cost markets
- World markets for resources and some products continue to develop
- Regulatory and legal environments become more uniform, but more complex (operational regulation is growing very fast)
- Convergence of global Financial and Technology markets and products continues

These trends all point to a high growth in volume of transaction most business are/going to experience

Convergence



Security Administration; Risk Discussion

- Definition of Risk (it is about data/information & processes)
  - Hard to define but the attributes are generally acknowledged
  - Stuff happens, what can go wrong will
  - Risk is generally caused by un-planed events
    - External and/or Internal
    - Known or recognized vs. unrecognized
- Organizational Impact
  - Quantitative
  - Qualitative
- Examples
  - Management, Transactional, Processing Failure, Interruption
  - Legal/environmental, Competition

Security Administration – Management

- Planning
  - Strategic
  - Tactical
  - Budgeting
- Controlling
  - Development of controls
  - Control monitoring
- Directing
  - Personnel supervision
  - Alignment of Accountability and Responsibility
- Organizing
  - Operational (with in IT & the organization)
  - Reporting structure

Security Administration – Transactional

- Fraud
  - Internal
  - External (contractor failure, other agencies, etc.)
- Transaction System Corruption
  - New system installation
  - Change control failures
  - Unplanned large volume changes
- Business activity not included in transaction processing systems
  - Manual overrides
  - Unauthorized desk top processing

Security Administration – Processing Failure

- Software / Hardware failure
- Key personnel availability
  - Cross-training
  - Succession plans
- Control failure / breakdown
- Sabotage
  - Internal
  - External

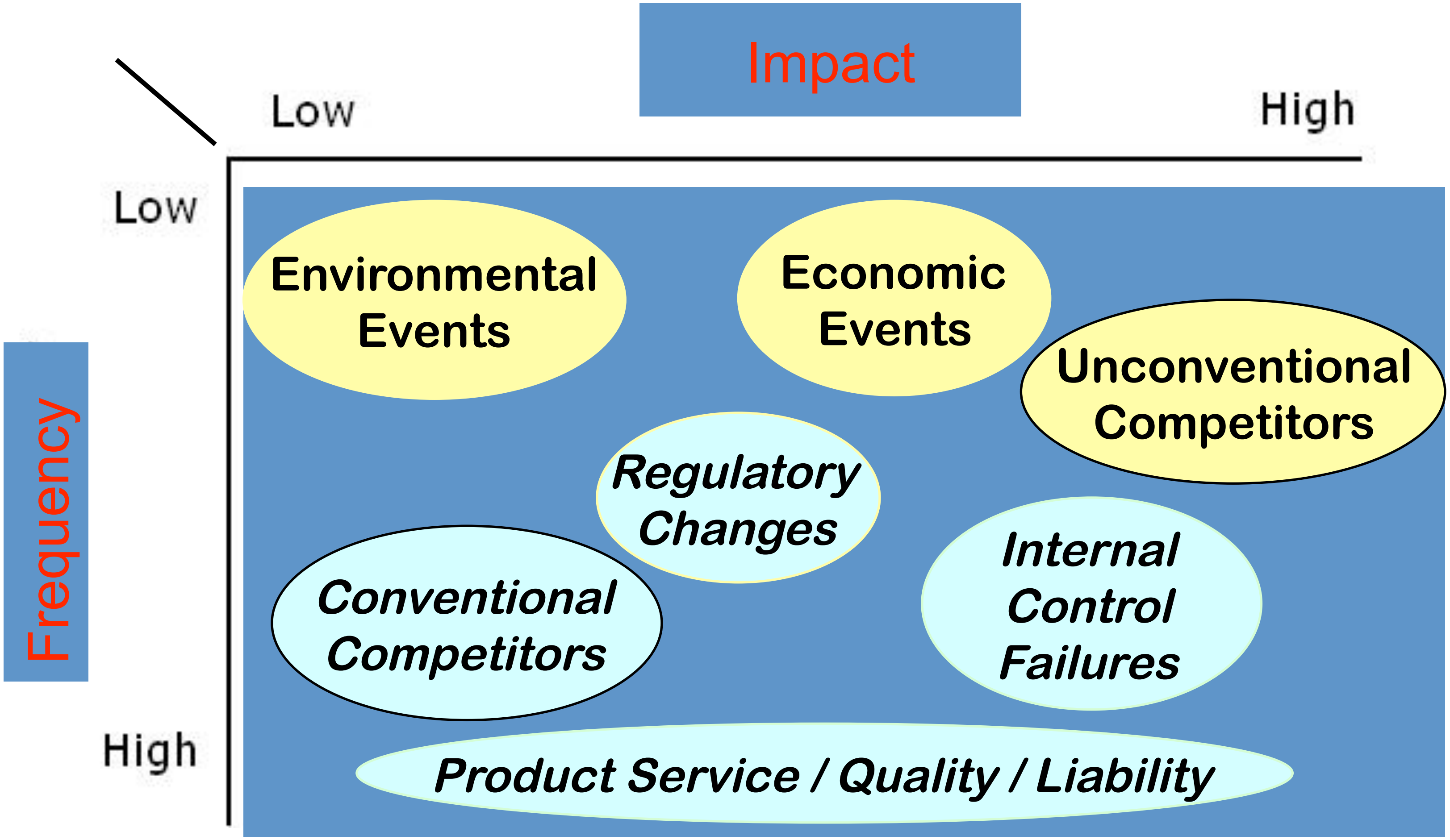
Security Administration - Interruption

- Vendor failure
- Internet services failure
- Data center/office or network hub failure
  - Acts of nature
  - Acts of man
- Cost (losses):
  - Tangible
  - Intangible

Security Administration – Legal /Environmental

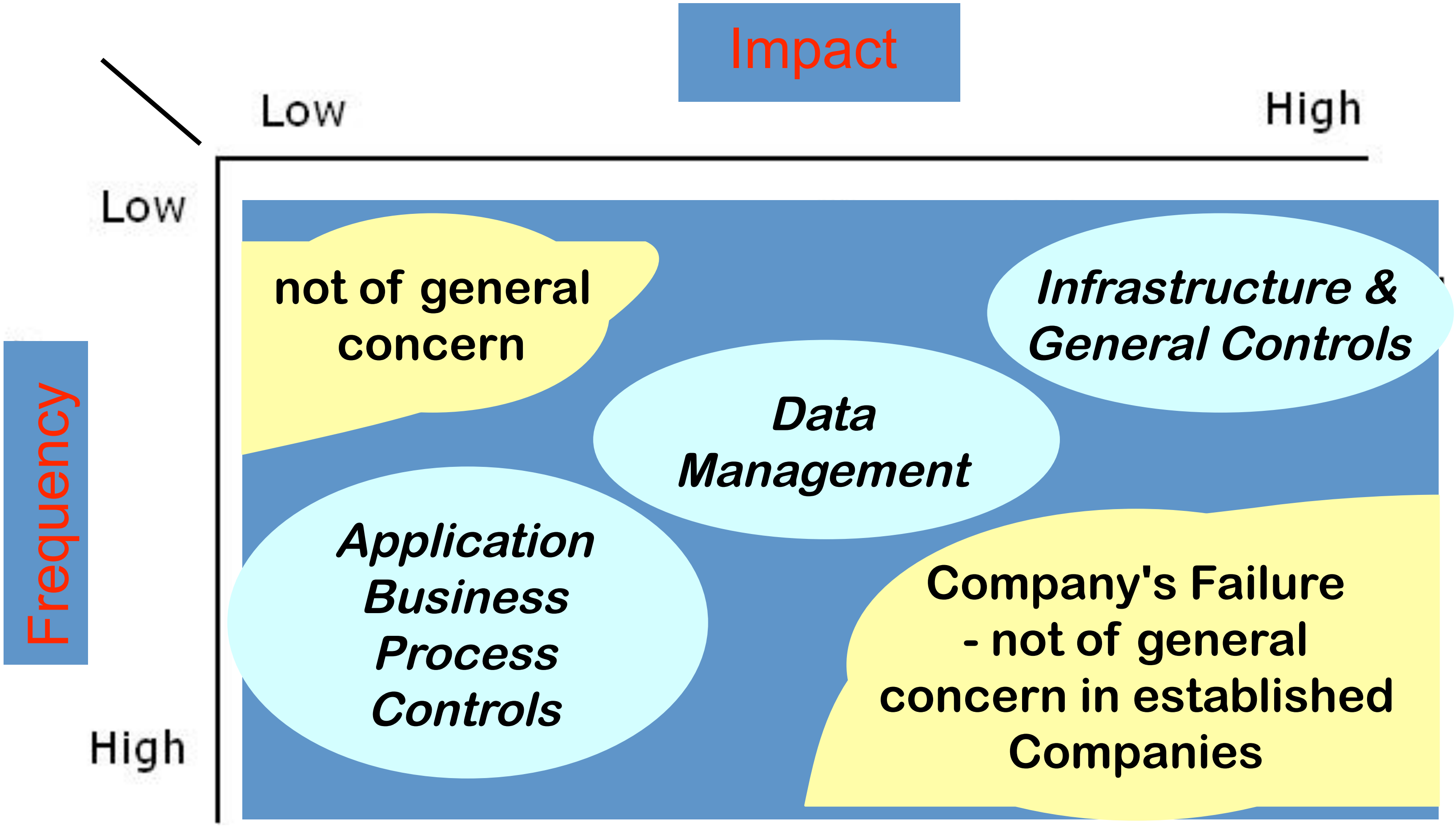
- Legal / Regulatory
  - Intellectual Property (IP)
  - Corporate legal frame work (regulatory compliance)
  - Not just are you in compliance but do you have proof of compliance
- Environmental
  - Product and/or environmental market loss
  - Legislative compliances/requirements

Business Value/Risks: Risk Model



ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Transactional (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

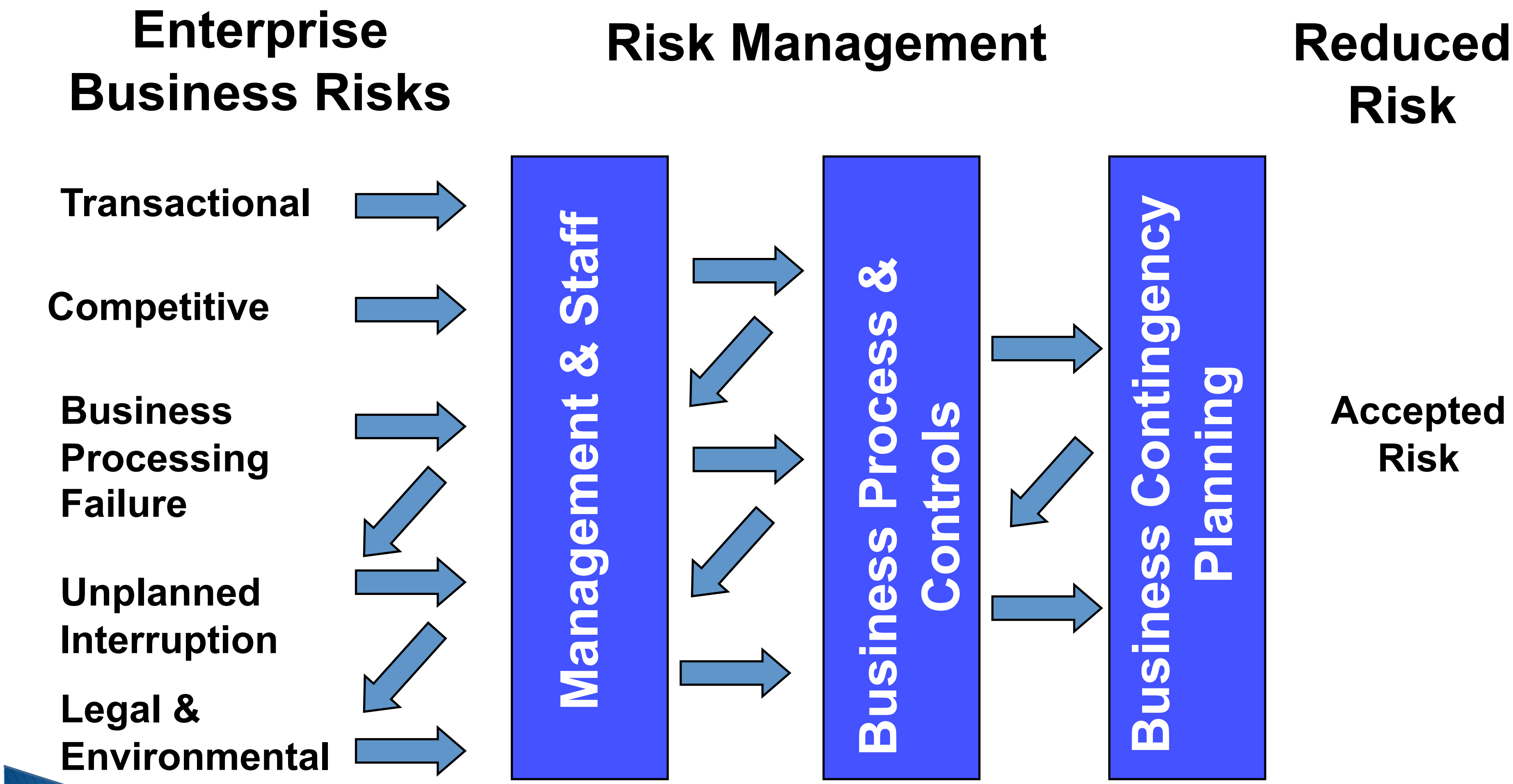
Risk Models – History's Lessons

- Organizational Risk
  - Unconventional competitor, Innovate or die
  - Product/Service levels can kill a company in today's global economy with record speed
  - Economic events and changes require planning (Periods of major changes creates big winners and big losers!)
- Transaction Risk
  - Must plan for the big events
  - Systems development and implementation is make or break
    - Systems for a strategic advantage in the market place
    - First mover advantage
    - New product or service

Risk and Controls Relationship

- Control Definition: Control is a management process to help/ support/achieve a desired result.
- Risk and Controls Relationship
  - Think of control as known risk abatement (process/event)
  - Some controls focus on a known risk only
    - Most accounting controls
    - Application controls
    - Regulatory compliance controls
  - Other controls focus on unknown risks, with a known results
    - DRP and BCP
    - Some information security controls
    - SDLC

Risk Management and Mitigation



Enterprise Business Risks

Risk Management

Reduced Risk

Transactional

Competitive

Business Processing Failure

Unplanned Interruption

Legal & Environmental

Management & Staff

Business Process & Controls

Business Contingency Planning

Accepted Risk

Transactional Risk - Low Volume

- Risk reduction is people dependent (get the required/correct intellectual capital on the task)
- Unique one time or limited in volume
  - M&A
  - New plant
  - Application development
  - New product/service introduction

Security Administration's role/involvement in low volume transactions is limited (in general) to data protection

Large Scale Transaction Processing

- Think of control as known risk abatement
- Automated and process controls must be dominate
- IT controls are most cost effective at known risk reduction
- Preventive controls are more cost effective than detective and/or corrective controls

Security Administration is a key part of not only data protection
but involved in the process controls that support the application's portfolio

Large Scale Transaction Processing

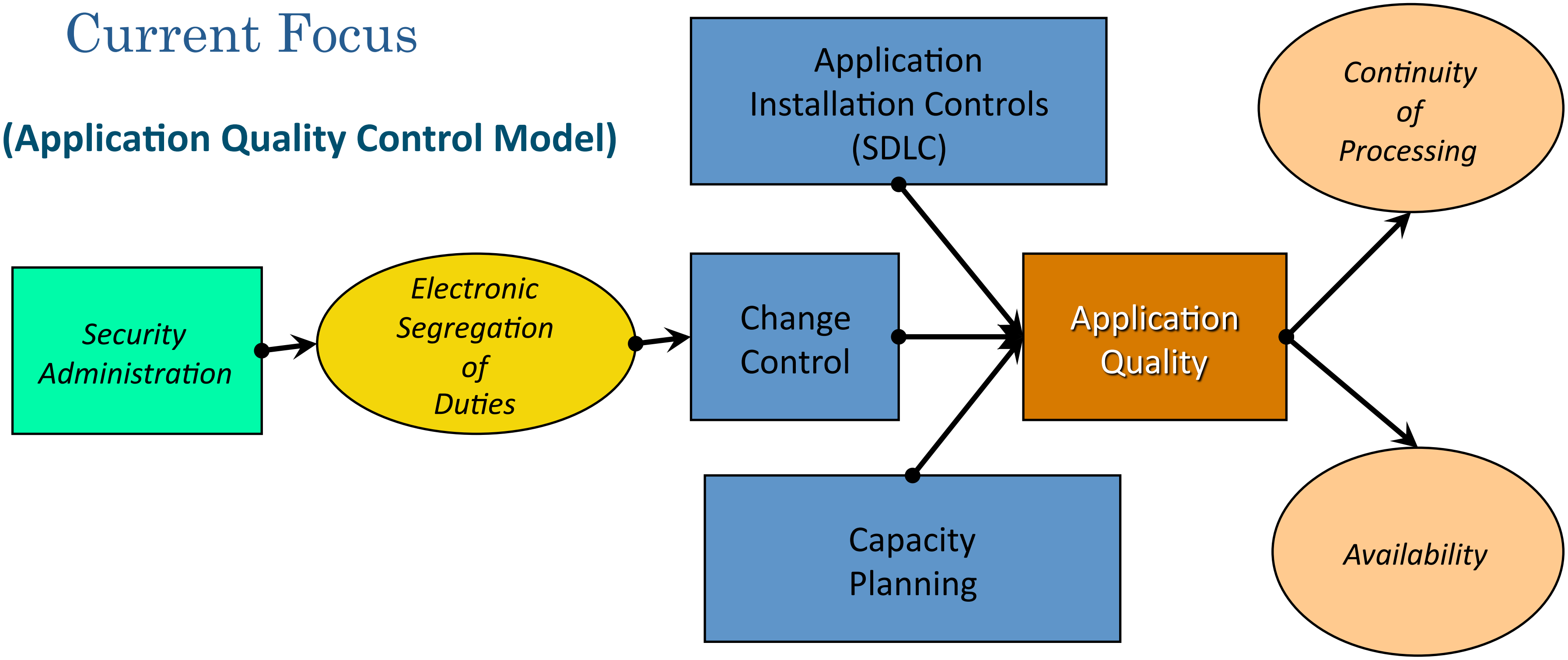
- As we move forward, ERP, CRM, CAD trends continue:
  - Users (e.g. accountants, engineers, sales force) define system-generated entries
  - System-generated entries are (or becoming) 90% of the total
  - Account analysis is system defined
  - Staffing effort is directed at the one-off (unique) transactions 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

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

IT Governance

Current Focus

(Application Quality Control Model)



Application Quality critically depends on the diligent exercise of Change Control

Organizational Impact

- Increasing transaction volumes
  - With mobile and dispersed workforce
  - With globally dispersed organizations
  - With globally expanding markets
- Diversifying base of technology
  - Increasing footprint for open source
  - Expanded channels of access, including mobile
  - Increasing complexity of solutions and technologies supporting them
- Expanding and complex global regulatory environment
  - Increasing regulatory requirements for tighter demonstrable and documented controls
  - Increasing complexity of regulatory reporting
  - Constantly changing regulatory landscape

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

IT Governance – Security Administration

- Electronic Assets that require protection are expanding rapidly
- Regulator changes are increasing the cost and the risk of nonperformance
- 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 IT & security administration role of "keeping the bad guys out" needs to change to "helping control business applications"

ISACA® Serving IT Governance Professionals San Francisco Chapter

Conclusions - Organizational

- 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.
- As transaction volumes grow, organizations place increasing reliance on the quality of their application portfolio. Measuring quality and setting goals should be considered.
- Regulatory changes in all major markets is a given. Quality in process and business function will aid in achieving compliance (time and money).
- The alignment of accountability and responsibility requires electronic segregation of duties in the pure electronic work environment.
- Electronic segregation of duties and personnel management controls are the only real controls in the electronic work space.
- Given the staffing to transaction ratio and that staff is organized to manage the application portfolio and timely recoverability is critical.

Conclusions – Internal Audit

- Security Administration should be viewed as a business with business processes (managed and audited as such).
- Management has heard about the bad guys long enough, discussions about how we run and management our business in the electronic work space may be appropriate.
- With a focus on change control of high volume applications, the value of application test data needs to be reviewed (several organization now protect and back this data with production data status).
- Application testing environments (including access controls) is critical to the change control process and should be in scope of audits.
- Audit risk analysis needs to consider application portfolio considerations

?

Thank You

ISACA®
Serving IT Governance Professionals
San Francisco Chapter