G23 - Building a Sustainable IT Compliance Program

Chong Ee

\

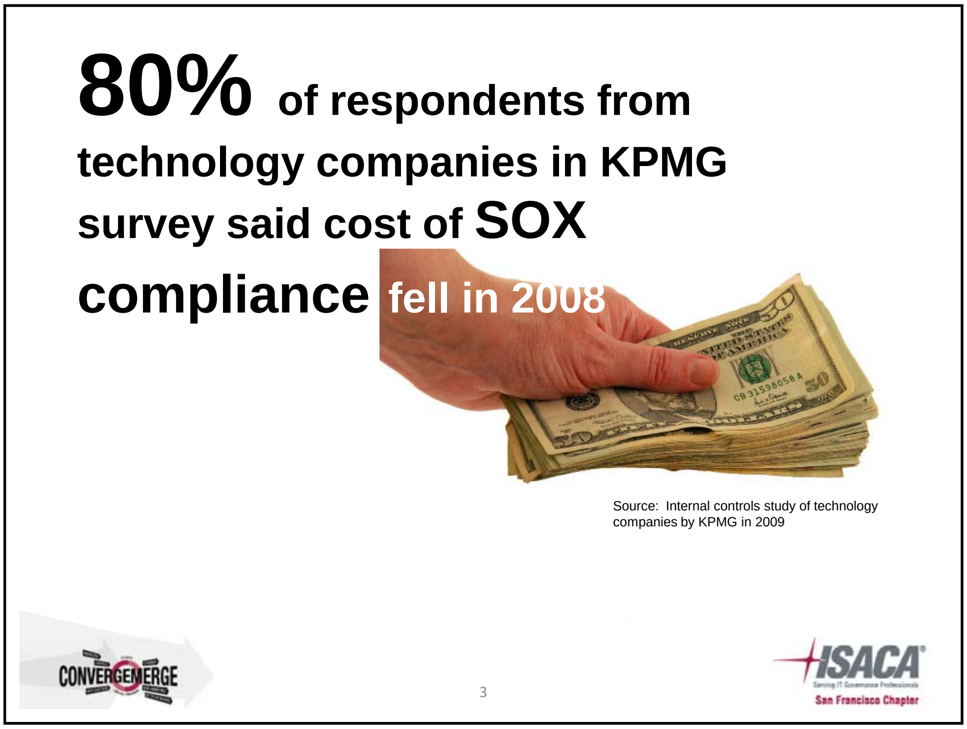
Building a Sustainable IT Compliance Program

Chong Ee, CGEIT

September 21, 2009 – September 23, 2009

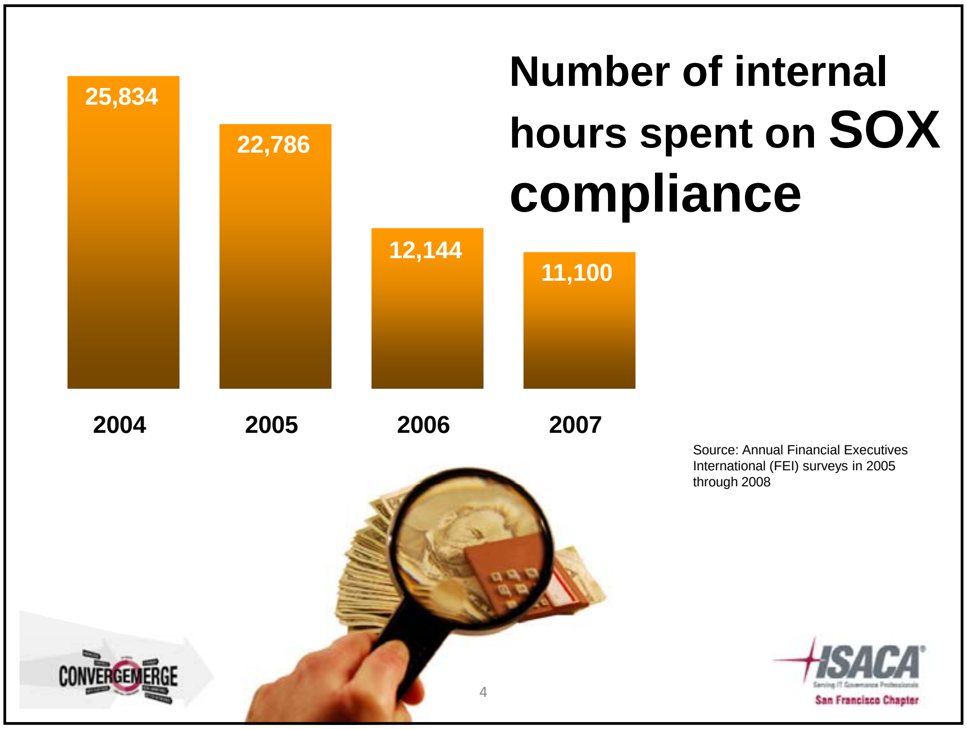
ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Building Compliance



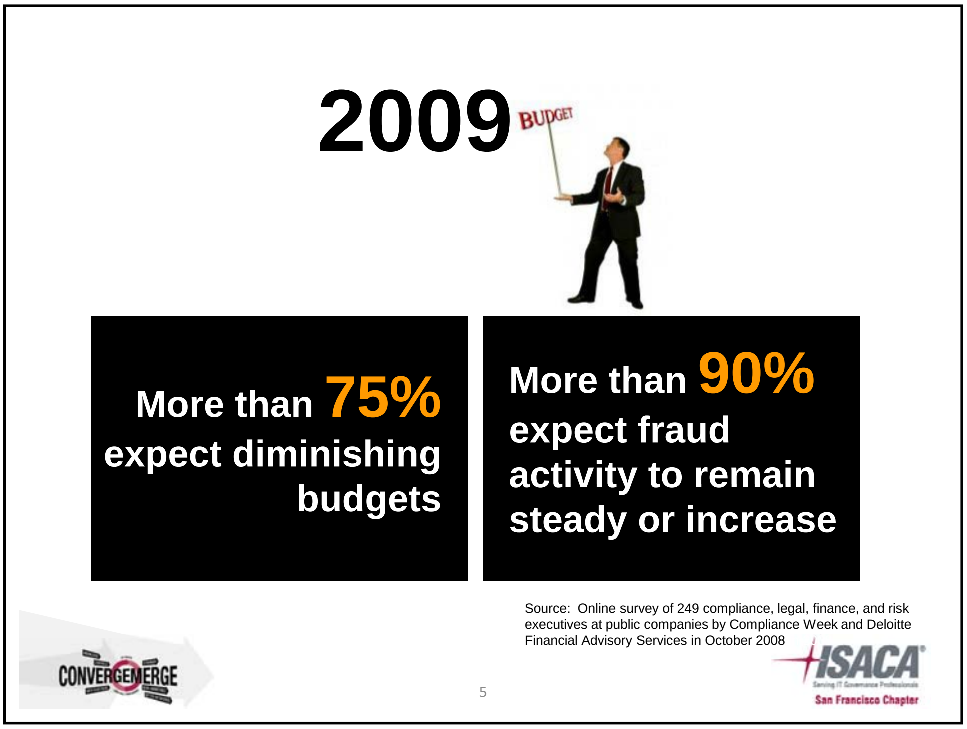
80% of respondents from technology companies in KPMG survey said cost of **SOX compliance** fell in 2008

Source: Internal controls study of technology companies by KPMG in 2009



Number of internal hours spent on SOX compliance

Source: Annual Financial Executives International (FEI) surveys in 2005 through 2008

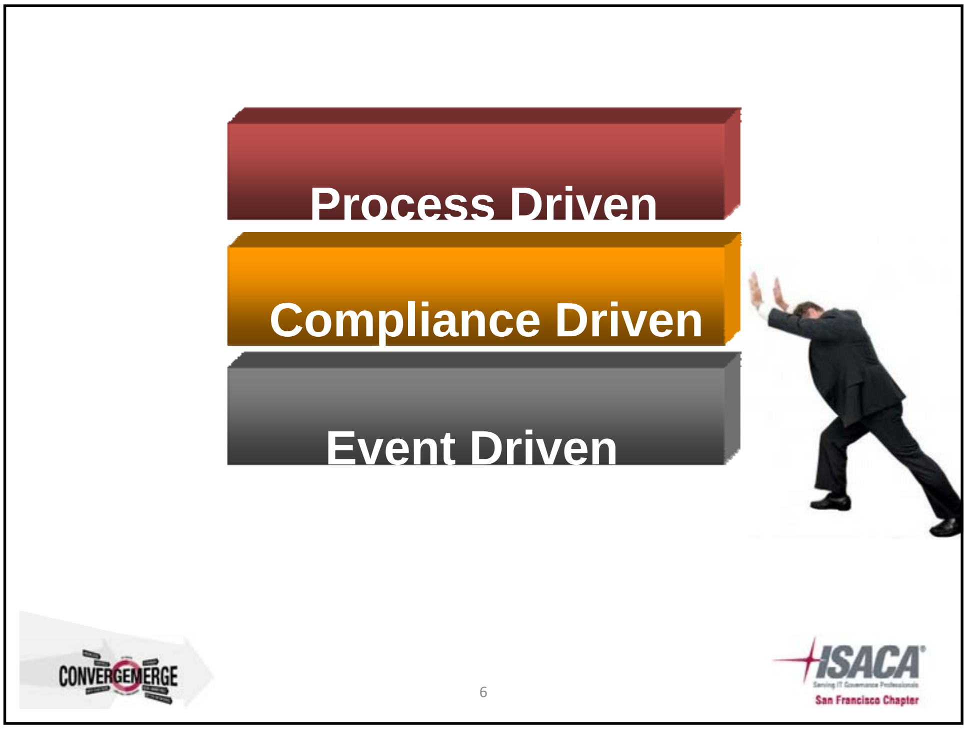


2009

More than **75%** expect diminishing budgets

More than **90%** expect fraud activity to remain steady or increase

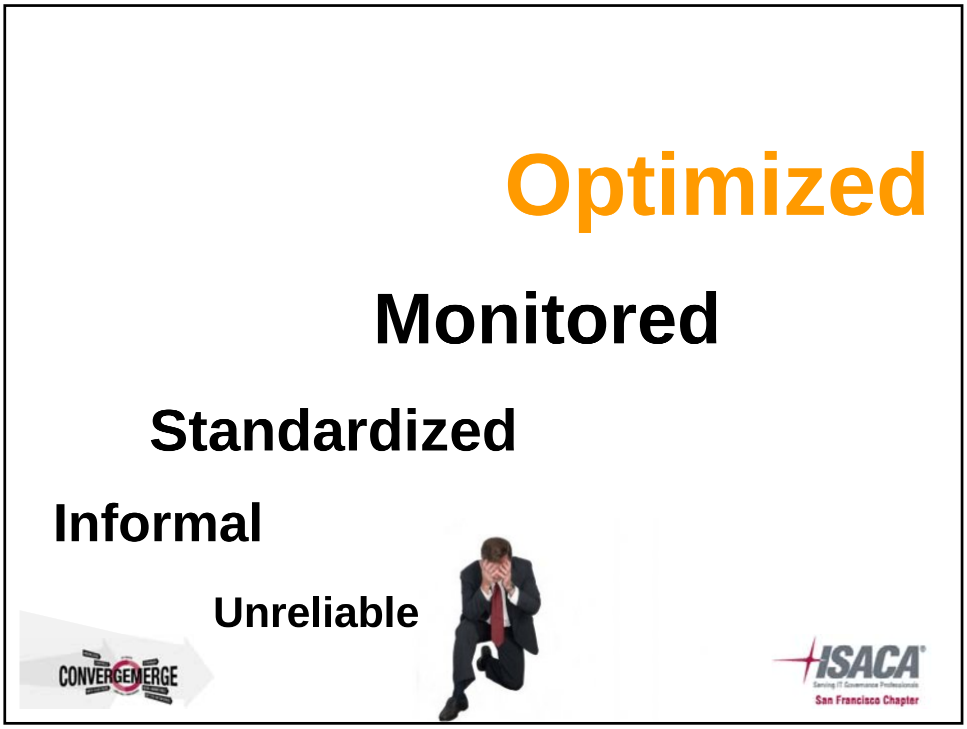
Source: Online survey of 249 compliance, legal, finance, and risk executives at public companies by Compliance Week and Deloitte Financial Advisory Services in October 2008



Process Driven

Compliance Driven

Event Driven



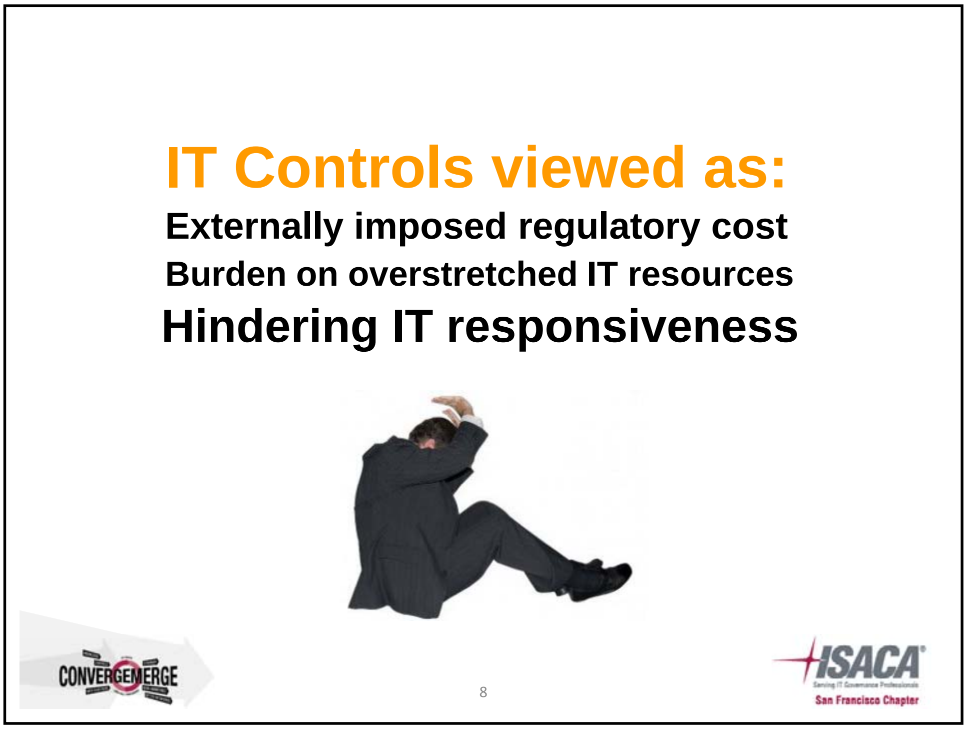
Optimized

Monitored

Standardized

Informal

Unreliable

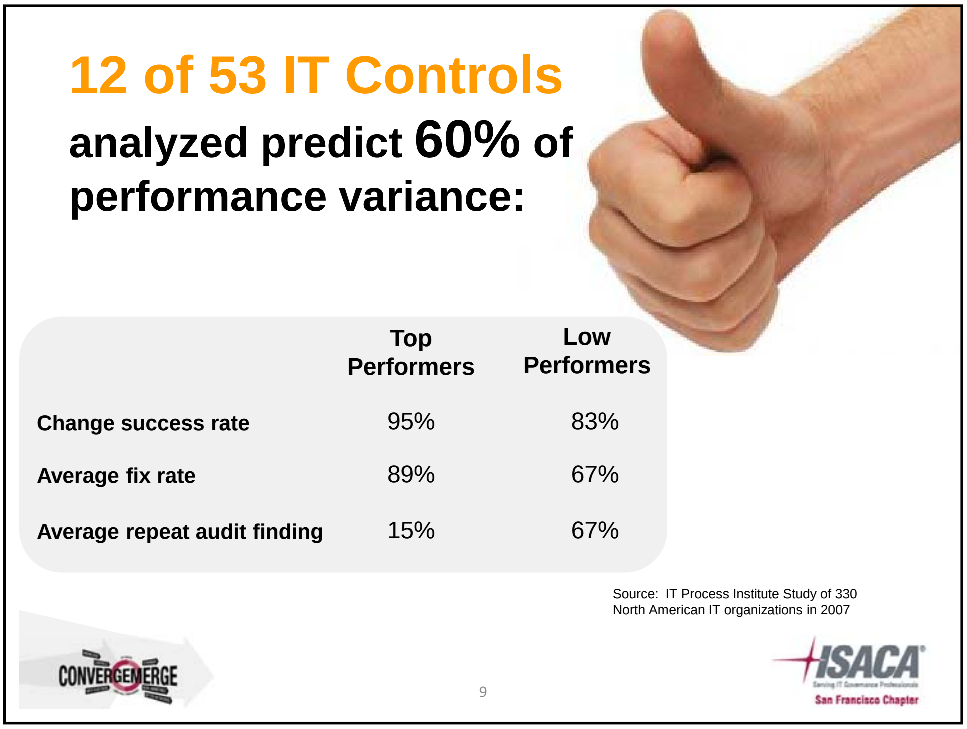


IT Controls viewed as:

Externally imposed regulatory cost

Burden on overstretched IT resources

Hindering IT responsiveness



12 of 53 IT Controls

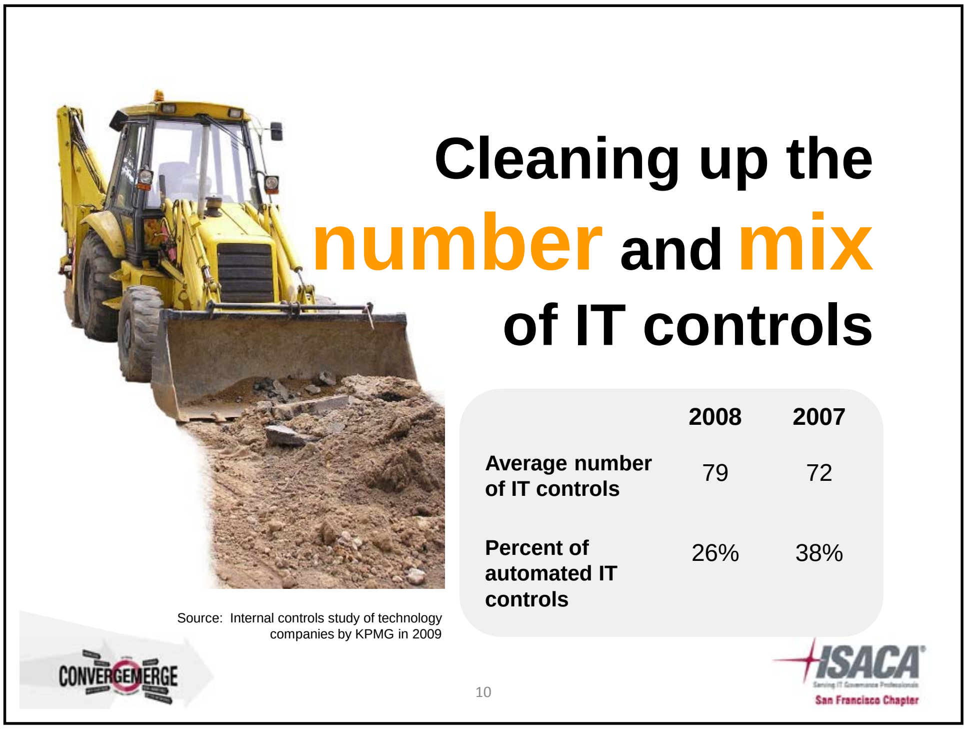
analyzed predict 60% of performance variance:

	Top Performers	Low Performers
Change success rate	95%	83%
Average fix rate	89%	67%
Average repeat audit finding	15%	67%

Source: IT Process Institute Study of 330 North American IT organizations in 2007

CONVERGEMERGE

ISACA San Francisco Chapter



Cleaning up the number and mix of IT controls

	2008	2007
Average number of IT controls	79	72
Percent of automated IT controls	26%	38%

Source: Internal controls study of technology companies by KPMG in 2009

CONVERGEMERGE

ISACA San Francisco Chapter

Automated versus Manual Controls

Prevention over Detection

Reliability over Error

Test of one over Test of Many

CONVERGEMERGE

ISACA
Serving IT Governance Professionals
San Francisco Chapter

Who is Responsible?

CONVERGEMERGE

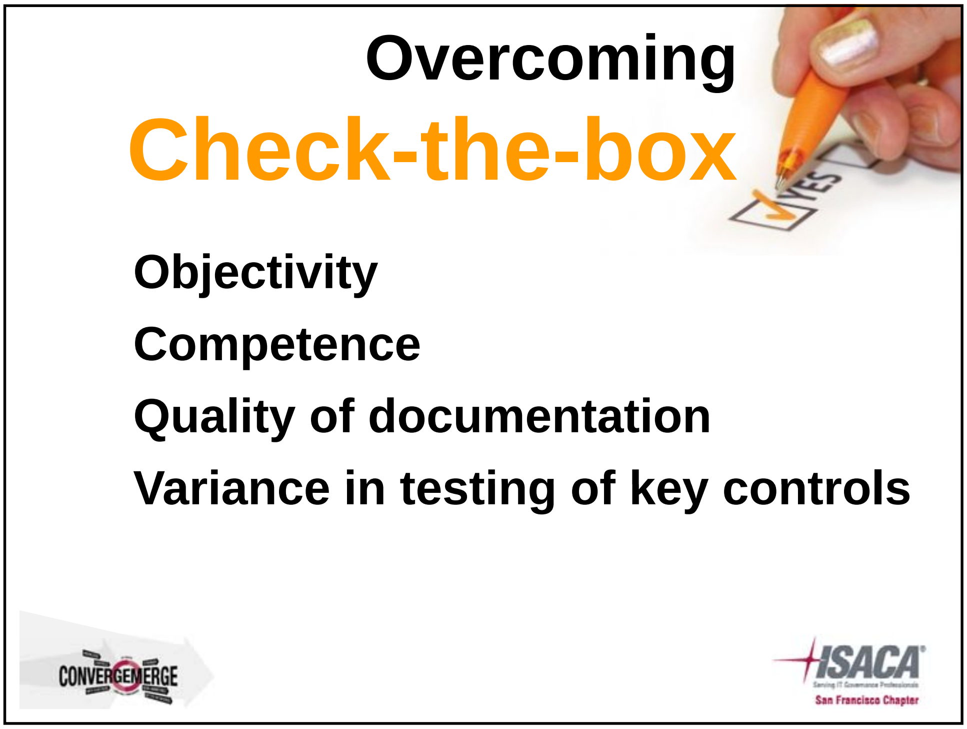
ISACA
Serving IT Governance Professionals
San Francisco Chapter

Training

Job Description

Management Oversight

Performance Evaluation



Overcoming

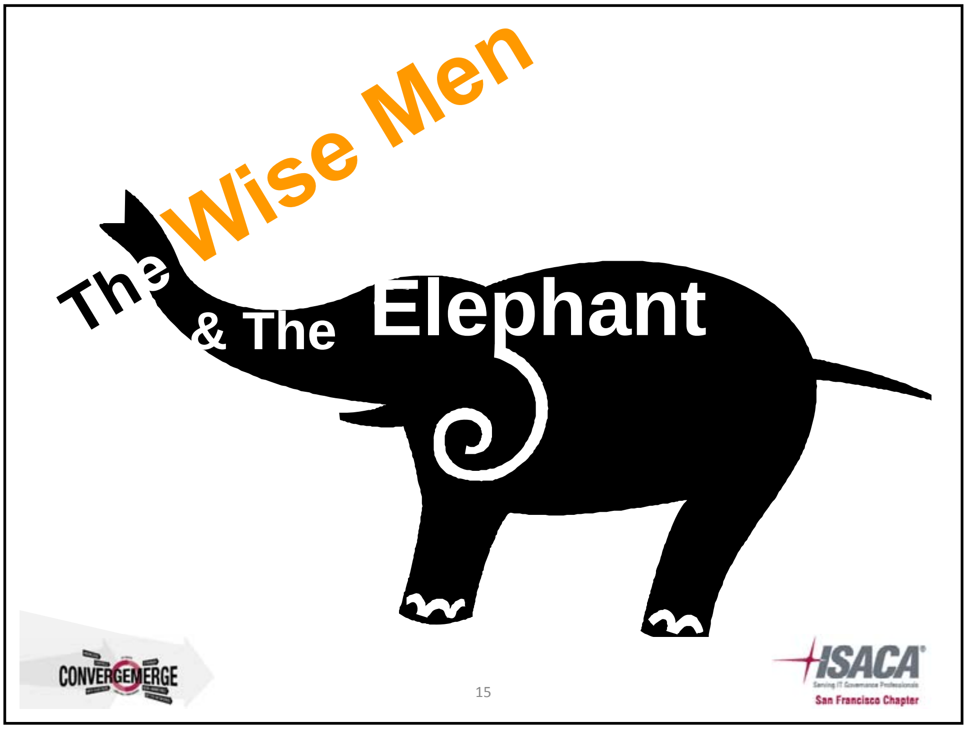
Check-the-box

Objectivity

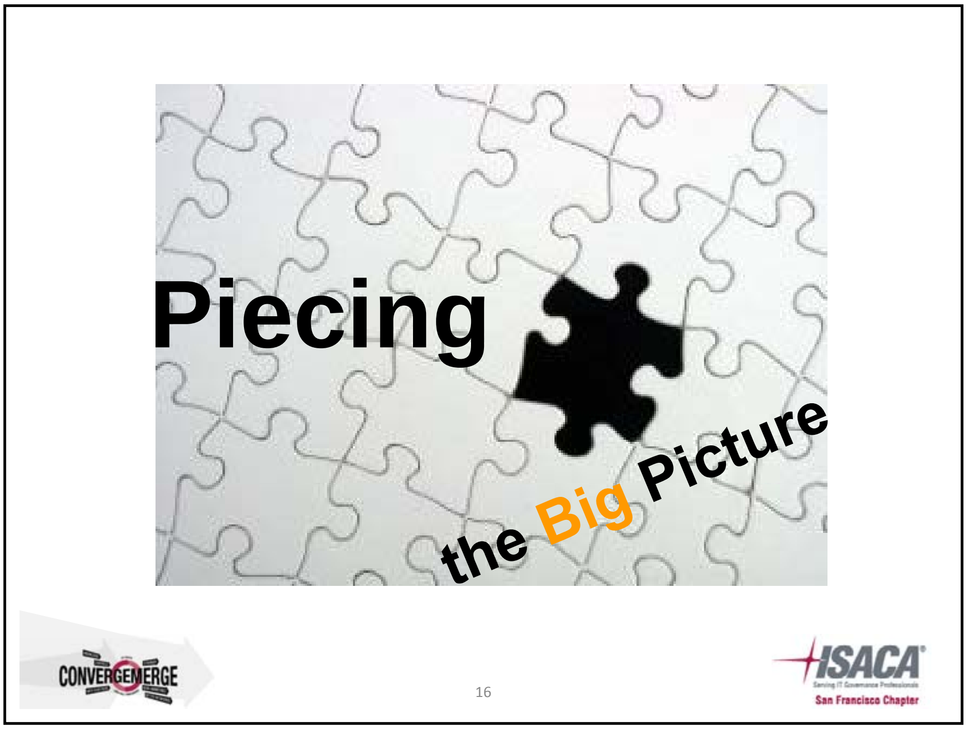
Competence

Quality of documentation

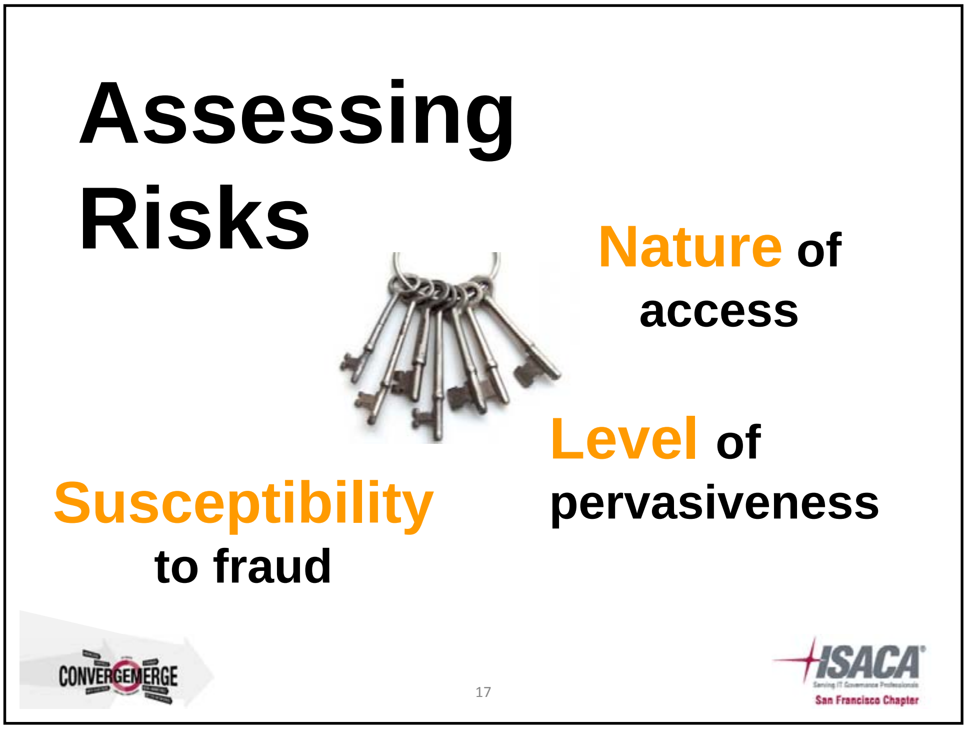
Variance in testing of key controls



The Wise Men & The Elephant



Piecing the Big Picture

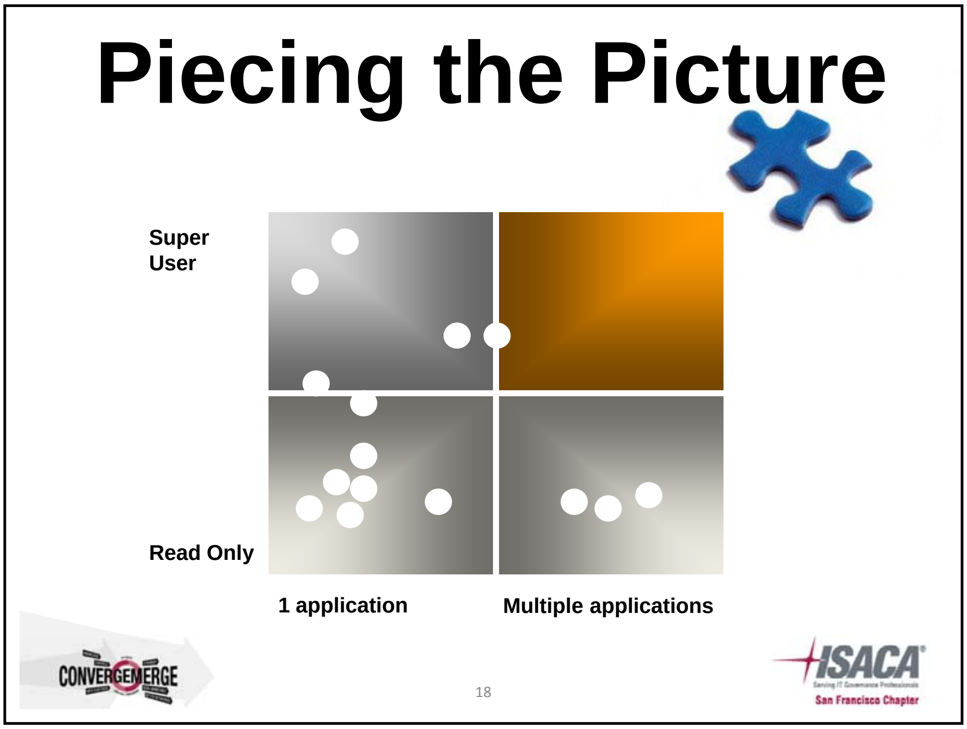


Assessing Risks

Nature of access

Level of pervasiveness

Susceptibility to fraud

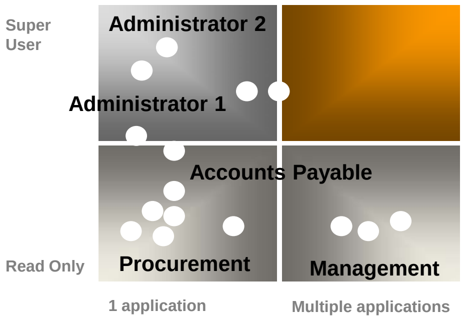


Piecing the Picture

Overlaying

Segregation of Duties

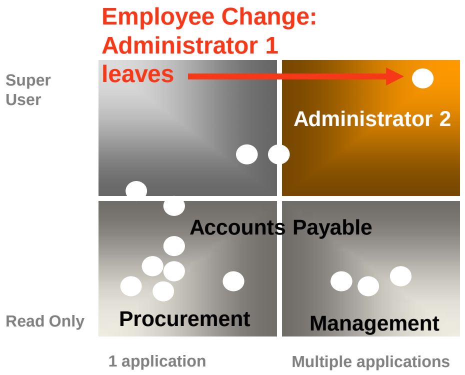
Compensating Controls



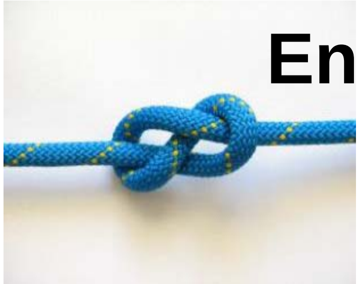
Managing

Potential Breaks

in Process



Mapping Systems



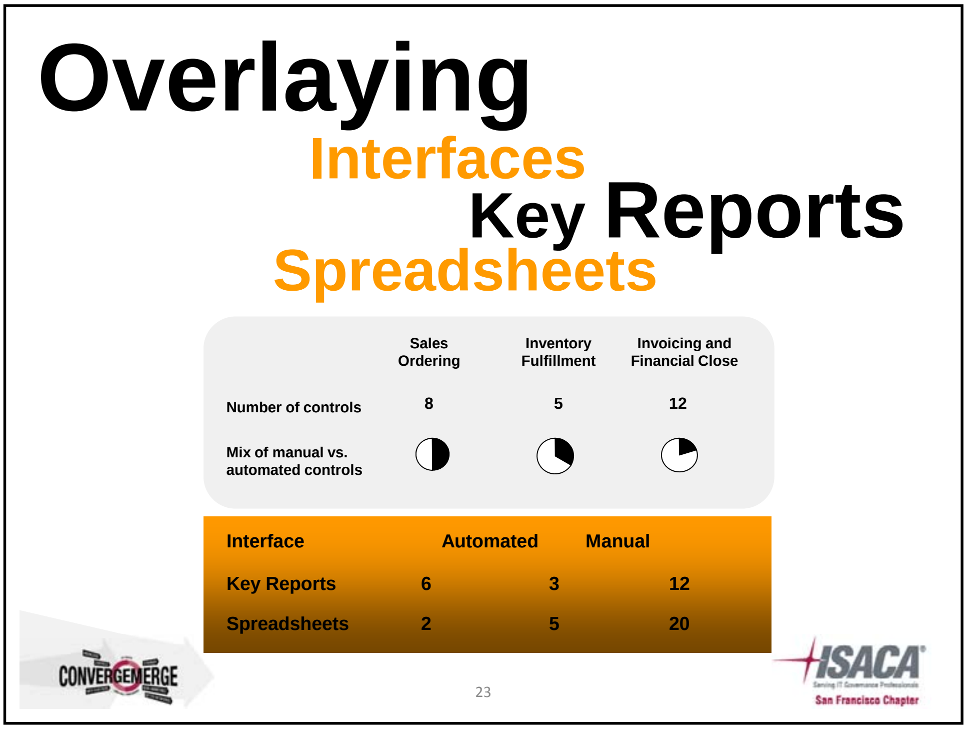
End to End

Distribution of controls

Mix of manual vs. automated controls

Piecing the Picture

	Sales Ordering	Inventory Fulfillment	Invoicing and Financial Close
Number of controls	8	5	12
Mix of manual vs. automated controls	◑	◔	◔



Overlaying

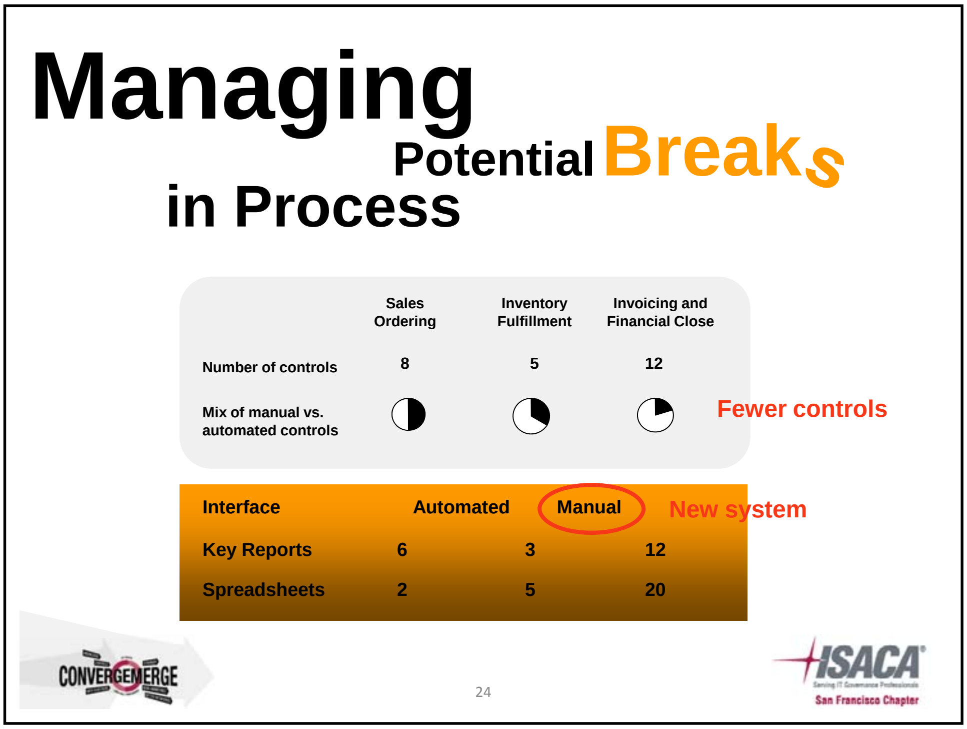
Interfaces

Key Reports

Spreadsheets

	Sales Ordering	Inventory Fulfillment	Invoicing and Financial Close
Number of controls	8	5	12
Mix of manual vs. automated controls	◑	◔	◔

Interface		Automated	Manual
Key Reports	6	3	12
Spreadsheets	2	5	20



Managing

Potential Breaks

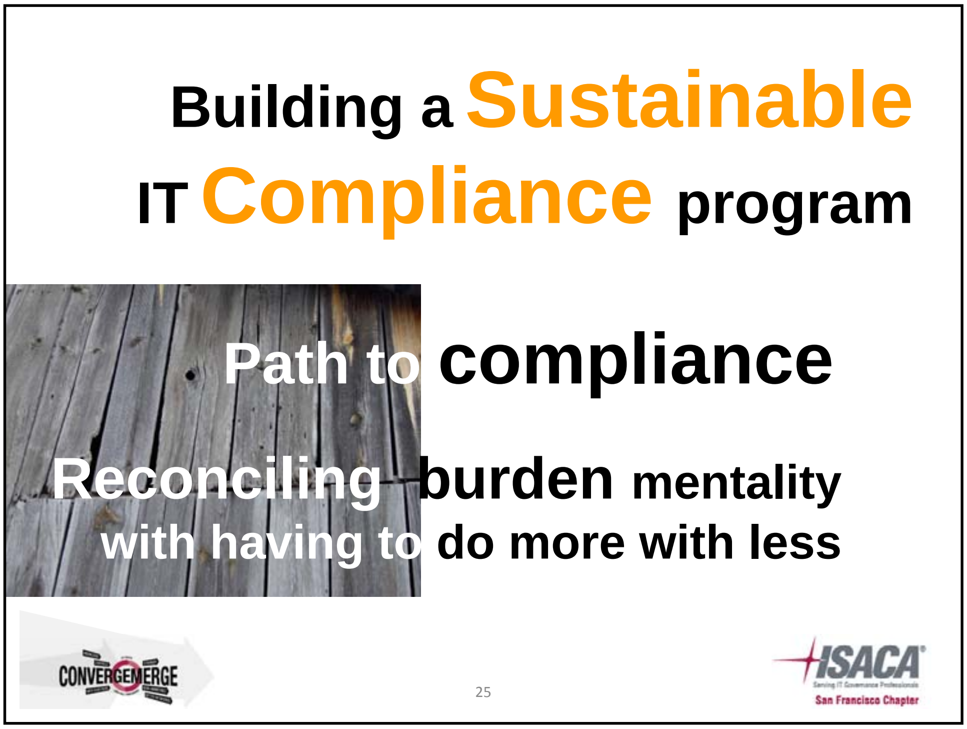
in Process

	Sales Ordering	Inventory Fulfillment	Invoicing and Financial Close
Number of controls	8	5	12
Mix of manual vs. automated controls	◑	◔	◔

Fewer controls

Interface		Automated	Manual
Key Reports	6	3	12
Spreadsheets	2	5	20

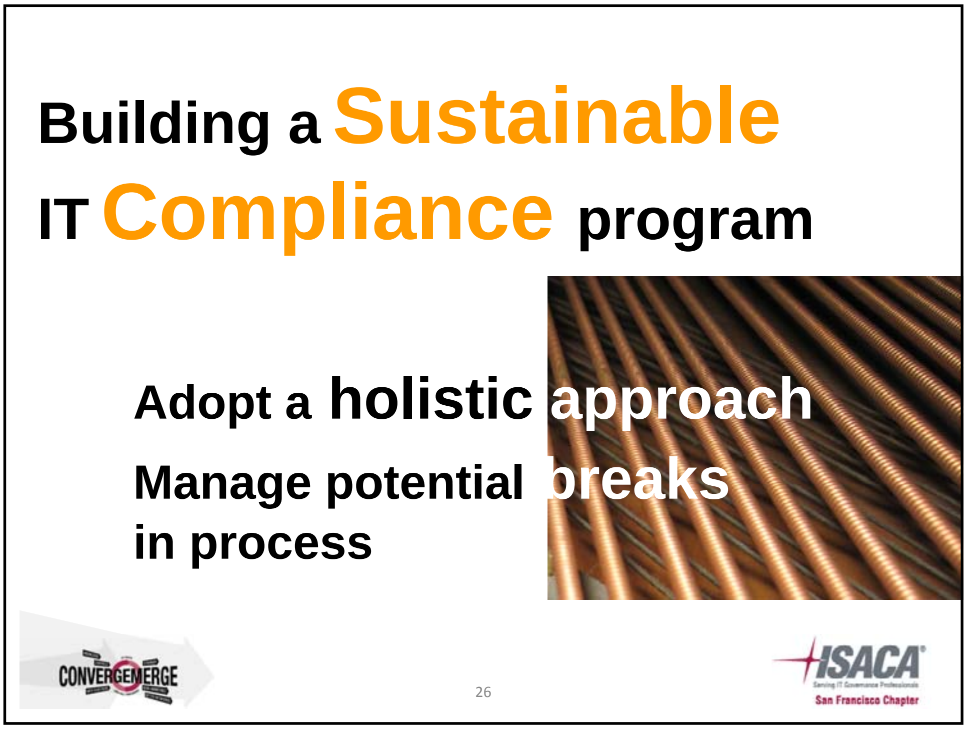
New system



Building a Sustainable IT Compliance program

Path to compliance

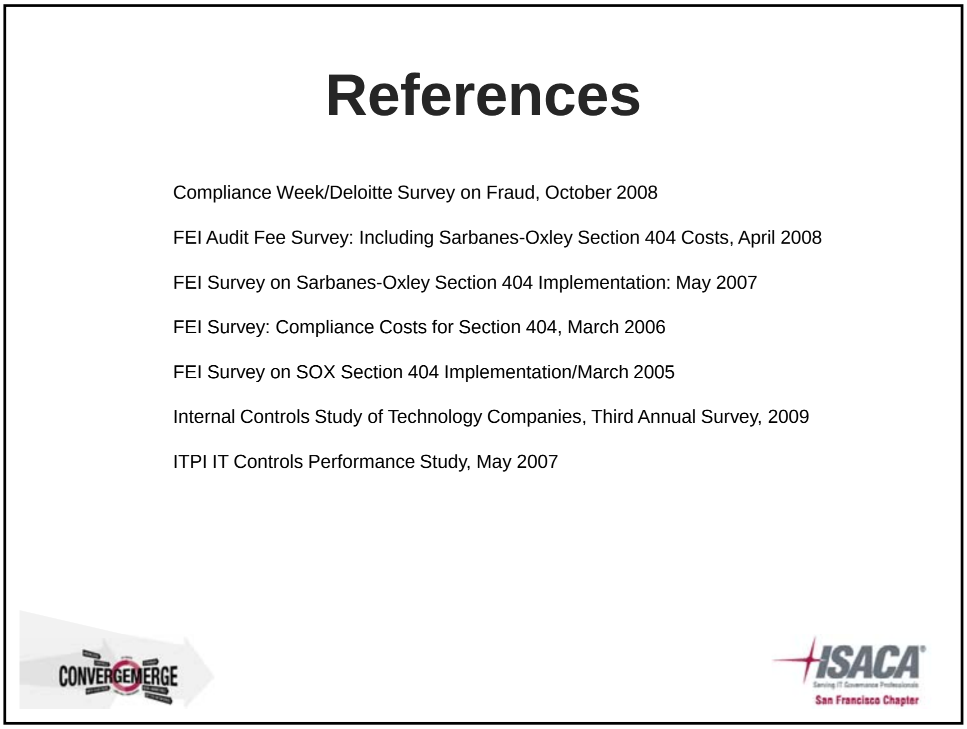
Reconciling burden mentality with having to do more with less



Building a Sustainable IT Compliance program

Adopt a holistic approach

Manage potential breaks in process



References

Compliance Week/Deloitte Survey on Fraud, October 2008

FEI Audit Fee Survey: Including Sarbanes-Oxley Section 404 Costs, April 2008

FEI Survey on Sarbanes-Oxley Section 404 Implementation: May 2007

FEI Survey: Compliance Costs for Section 404, March 2006

FEI Survey on SOX Section 404 Implementation/March 2005

Internal Controls Study of Technology Companies, Third Annual Survey, 2009

ITPI IT Controls Performance Study, May 2007