



# Ignorance is Risk

## Manage by Measurement Through the Use of a Control Framework

Jeromie Jackson- CISM, CISSP  
Security Solutions Architect  
Technology Integration Group (TIG)  
Jeromie.Jackson@tig.com  
858-205-3645- BB  
619-368-7353-cell



# Brief Bio.

- President- San Diego OWASP
- Vice President- San Diego ISACA
- CISM, CISSP Since 1996
- CISM, COBIT, & ITIL Certified
- SANS Mentor
- Security Solutions Architect @ TIG

## Articles

- \* Covered on Forbes Magazine
- \* Credit Union Business Magazine
- \* Credit Union Magazine
- \* CU Times
- \* Insurance & Technology Review
- \* CMP Media
- \* Storage Inc.

## Speaking Events

- \* SPC 2009
- \* SecureIT 2008
- \* SecureIT 2009
- \* Interop
- \* Government Technology Conference (GTC)
- \* Many Credit Union Leagues



# Risk is a Business Issue

“Ignoring or misunderstanding financial risks played a substantial role in creating the world financial crisis in 2008.”

“Organizations need to assess risk as part of cost-cutting decisions and should manage increased IT risks to prevent operation failures that will lead to further loss.”

- Gartner, “Managing IT Risks During Cost-Cutting Periods”, October 22, 2008

# Risk is a Business Issue (Cont.)

- CardSystems Solutions Inc.
  - Mid 2005 breach of 40 million credit cards.
  - Visa & Mastercard terminated their processing capability- they soon went under
  - 35+ million data records were breached in 2008 in the United States-Theft Resource Center
- Heartland Payment Systems
  - Jan 20, 2009
  - *100 Million Transactions Per Month*
  - *<http://www.2008breach.com>*
- 252,276,206 records with personal information since January 1995
  - <http://www.privacyrights.org>

# Risk Aware



**RISK ASSESSMENT**

It's Not Worth It

DIY.DESPAIR.COM

# Risk Adverse



# Risk Aware Vs. Risk Adverse

## Risk Aware

- OK to Talk About Risk
- Ok to Take Risks
- Ok to Fail (if managing appropriately)
- Success and failures tracked and analyzed
- Continuous learning and improvement for key processes
- Realistic budgets and time lines that are continuously monitored
- Enterprise is able to take on bigger risks

## Risk Adverse

- Avoids Discussions of Risk
- Avoids Responsibility for risks
- No tracking or Analysis of Features & Successes
- Can't Learn From Mistakes; High Repeat Failure Rates
- Padded Budgets, Extended Time Lines, Surprise Overruns
- Managers Assign Blame, Don't Share the Risk

2007 MIT Sloan Center for Information Systems Research & Gartner Inc.

***Being Risk Aware Enables Agility & Innovation***

# Regulation With Minimal Benefit

A person in a suit stands on a small pedestal in the center of the frame. Surrounding them are several large, stylized magnifying glasses of various sizes and orientations, some overlapping. The background is a textured, reddish-brown color. The overall image conveys the idea of being scrutinized or regulated excessively.

- **Redundant Requirements**
- **Controls without clear benefits**

- **Overlapping and vague requirements**
- **Costly resource allocation**

- **50 Case Studies**
- **130 Firms Surveyed**
- **2000+ Executives Refined**

## *The Root-Cause of IT Risk - Lack of Governance*



“..Manifested as uncontrolled complexity, and inattention to risk.”

George Westerman & Richard Hunter, *IT Risk; Turing Business Threats Into Competitive Advantage*  
(Harvard Business School Press, 2007)

**Governance- “Specifying the decision rights and accountability framework to encourage desirable behavior in using IT.”**

- Peter Weill and Jeanne Ross, *IT Governance: How Top Performers Manage IT Decisions Rights for Superior Results*  
(Boston: Harvard Business School Press, 2004)

# Governance

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



# Leading the Trauma Unit



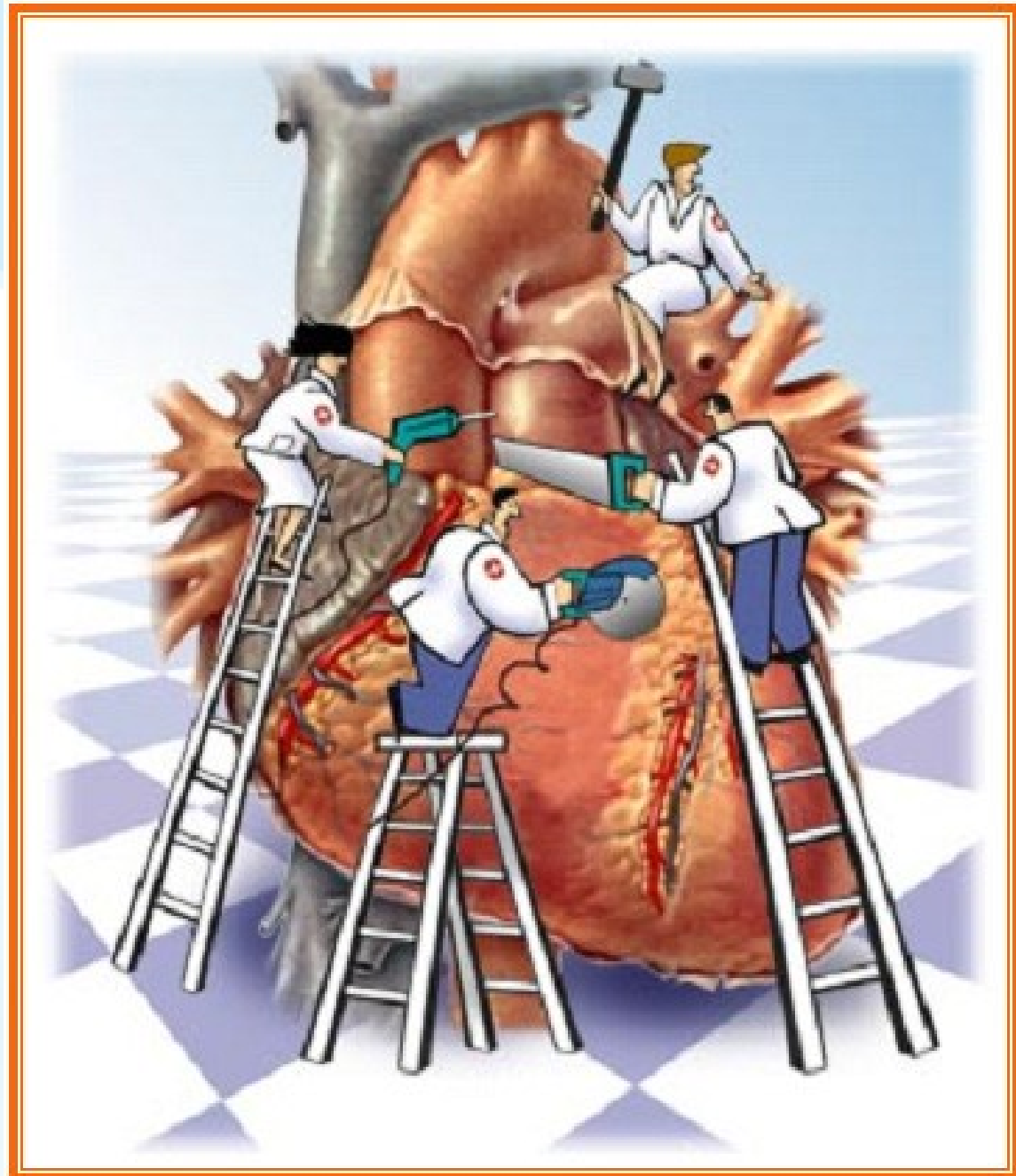
# Stop The Bleeding - Cauterize the Wounds

- Identify & Collect Known Risks
- Create a Remediation Portfolio
- Document the “As-Is” State

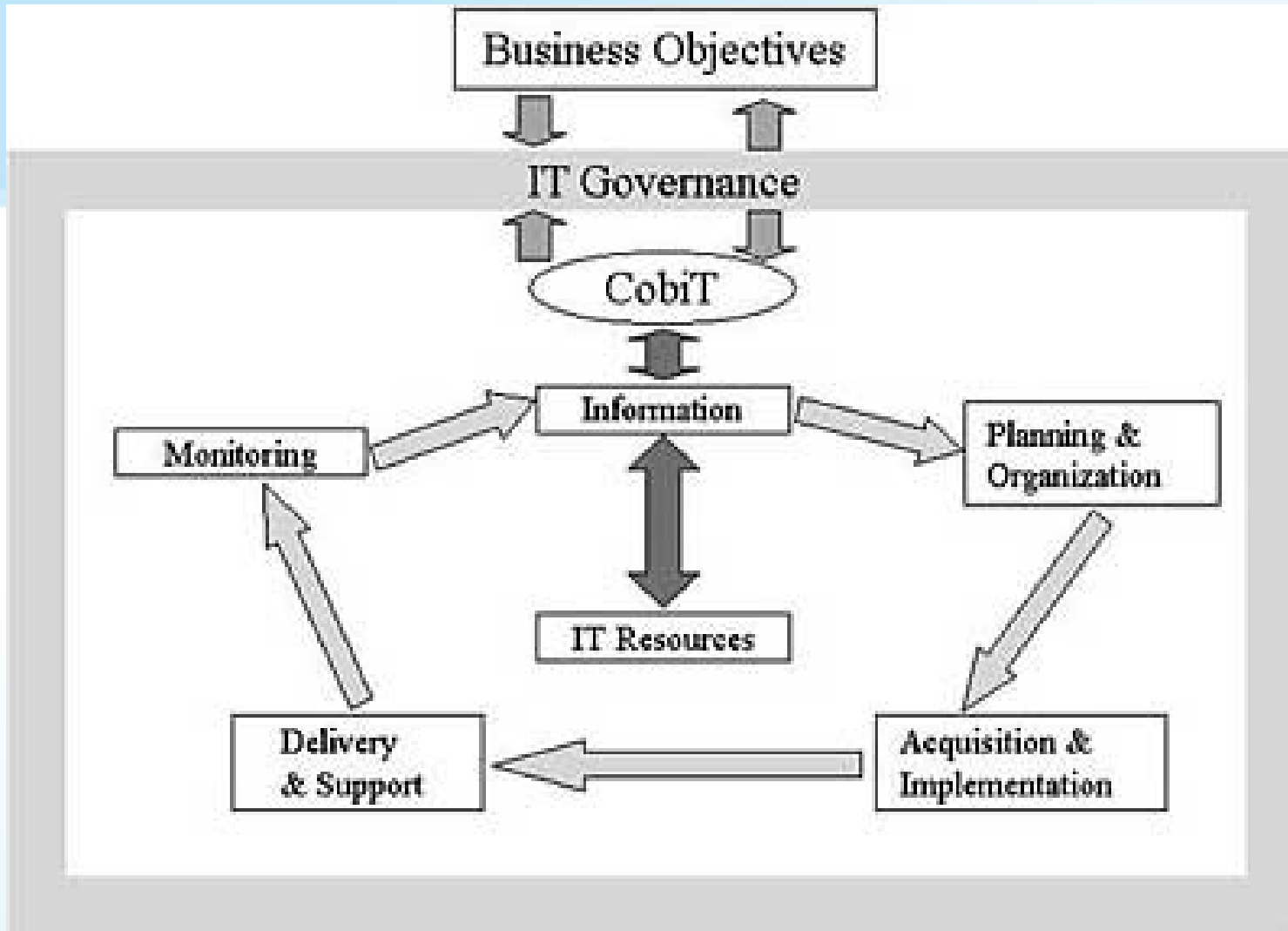


# Stabilize the Patient

- **Classify Known Risks**
  - External Audits
  - Internal Audits
  - Regulatory Audits
  - Vulnerability Assessments
  - Risk Assessments
- **Address Availability**
  - Focus on Business Consequence
- **Consolidate Regulations**



# IT Assessment



# Common IT Audit Deficiencies

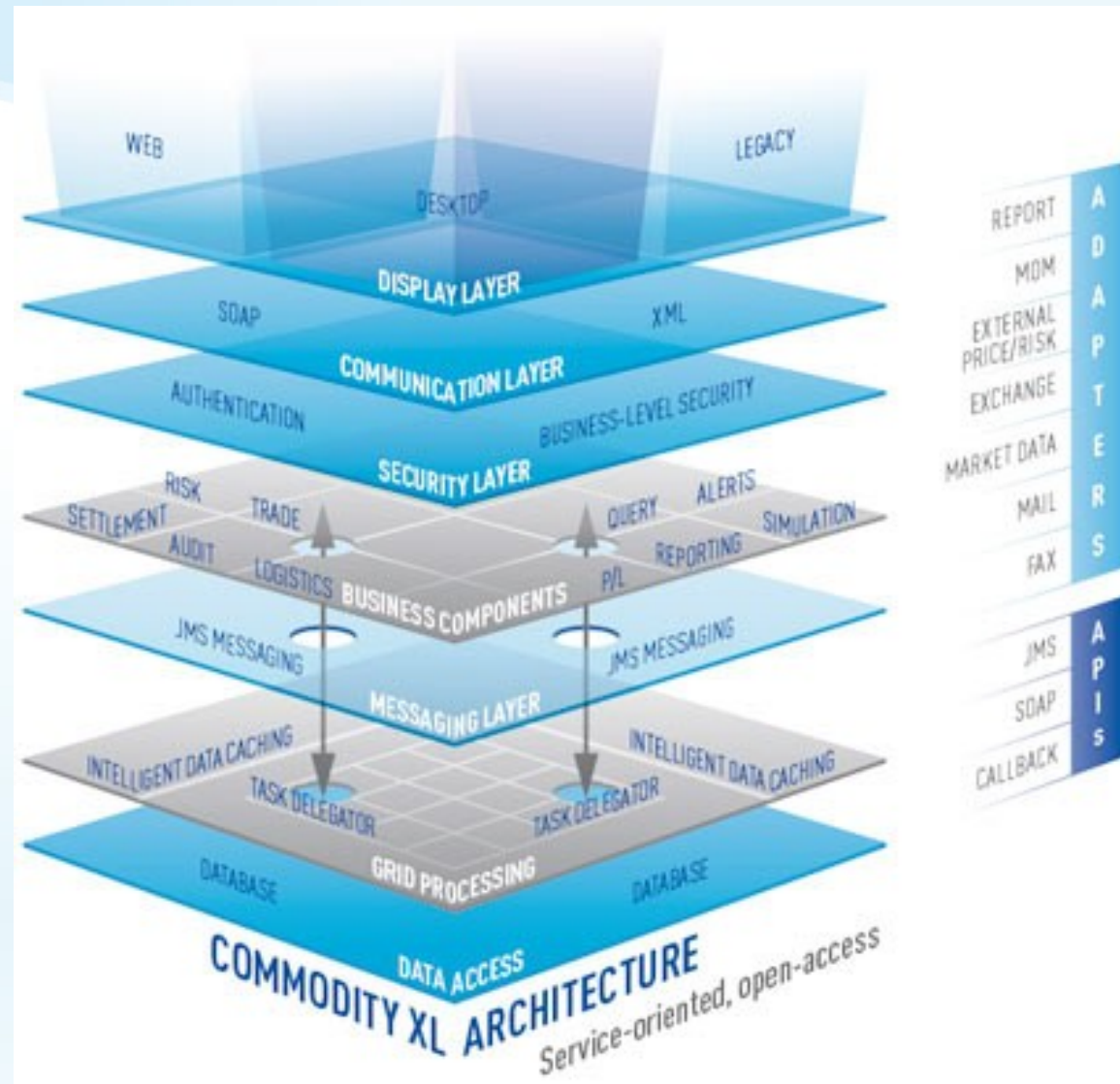
- Third-Party agreements and contracts weak
- Employee Awareness Training needed improvement
- Too many privileged accounts
- Inability to document user privileges
- Log collection weak
- Critical assets not clearly defined & documented
- DR/BCP not regularly tested
- Internal controls not routinely reviewed
- Change management documentation & consistency lacking
- ERP systems riddled with segregation issues

- Paul Proctor and Gartner Risk & Compliance Research Community, March 2007



# Have a clear architectural direction / “To-Be” state

- Conduct an IT Assessment to identify “As-Is” State
- Through planning identify core strategies and architecture
- Manage by Measurement



- **Optimize Remediation**
- **Assert Compliance Simultaneously**

**Regulatory Convergence**

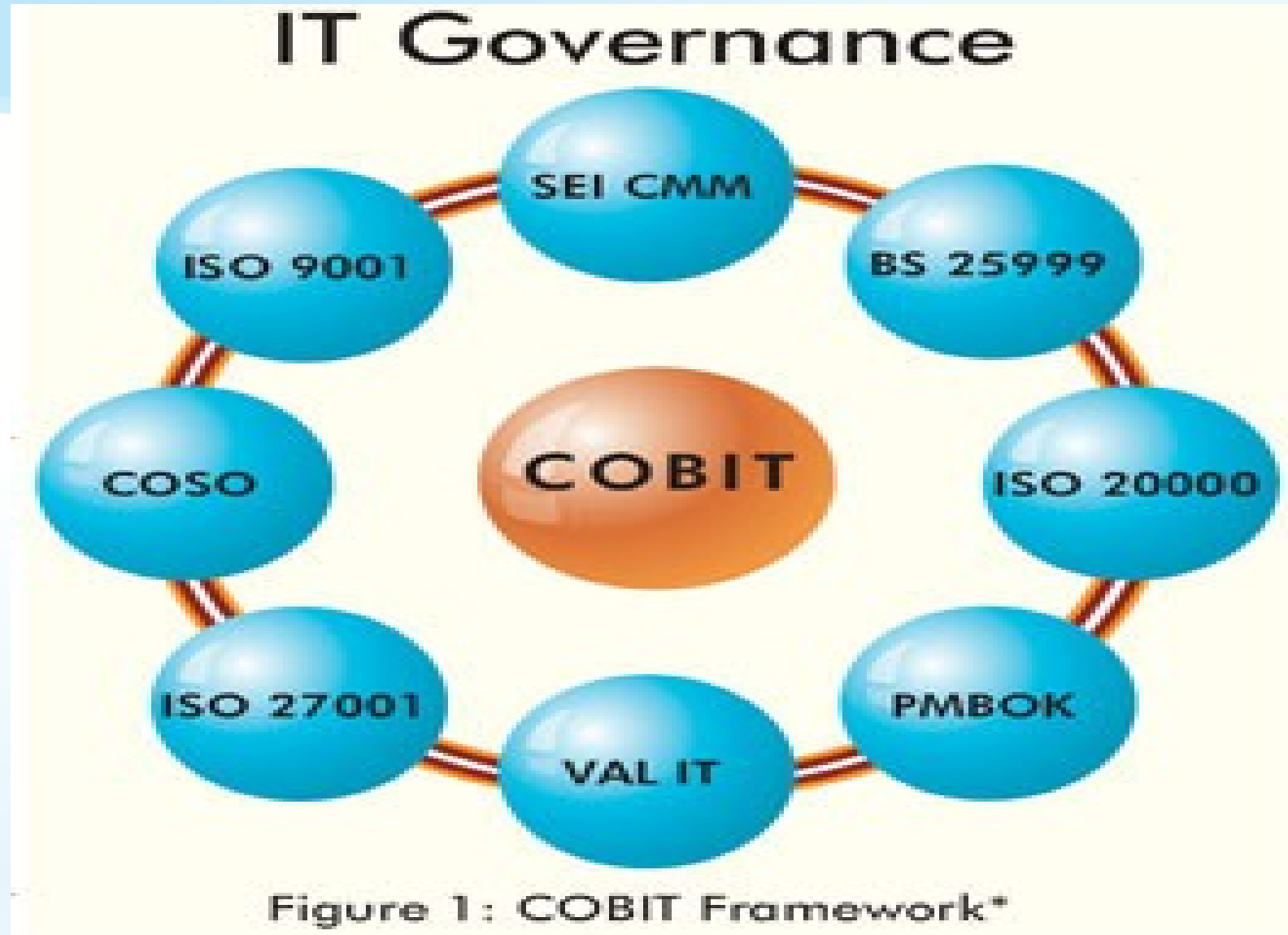


# Seek Optimal Treatment Plan

- Benefits of utilizing best practices
  - Enables external expertise
  - Facilitates benchmarking
  - Auditor familiarity resulting in reduced costs



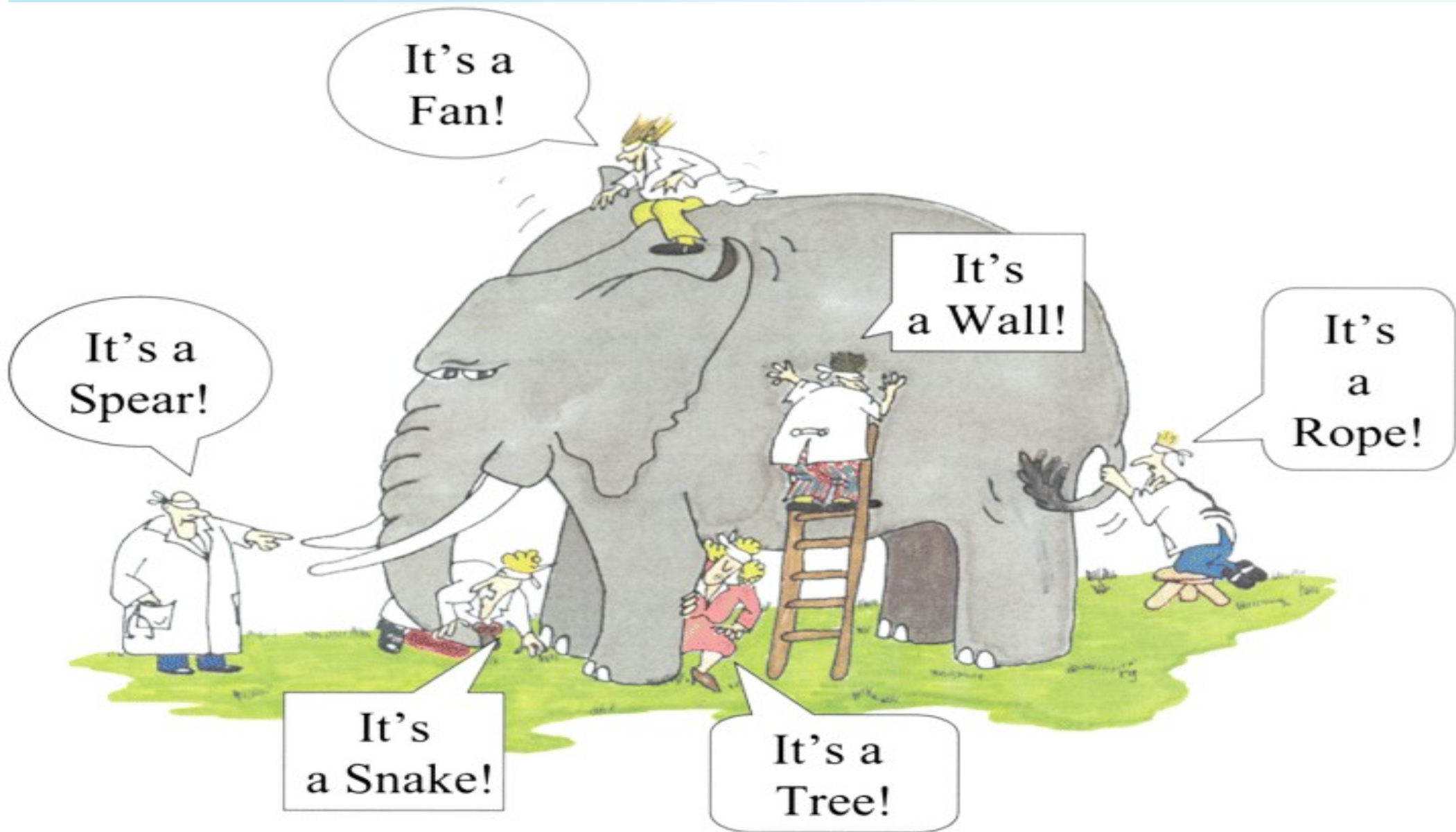
# Best Practice Control Objectives



# Components of Controls

- Defines a specific goal
- Aligns with business objectives
- Describes the focus required to manage
- Summarizes how the goal will be achieved
- Defines potential KPIs/KGIs
- RACI Table

# Communicate & Collaborate



- Paradigms- 7 Habits of Highly Effective People- "A man on a subway sees 2 obnoxious children..."

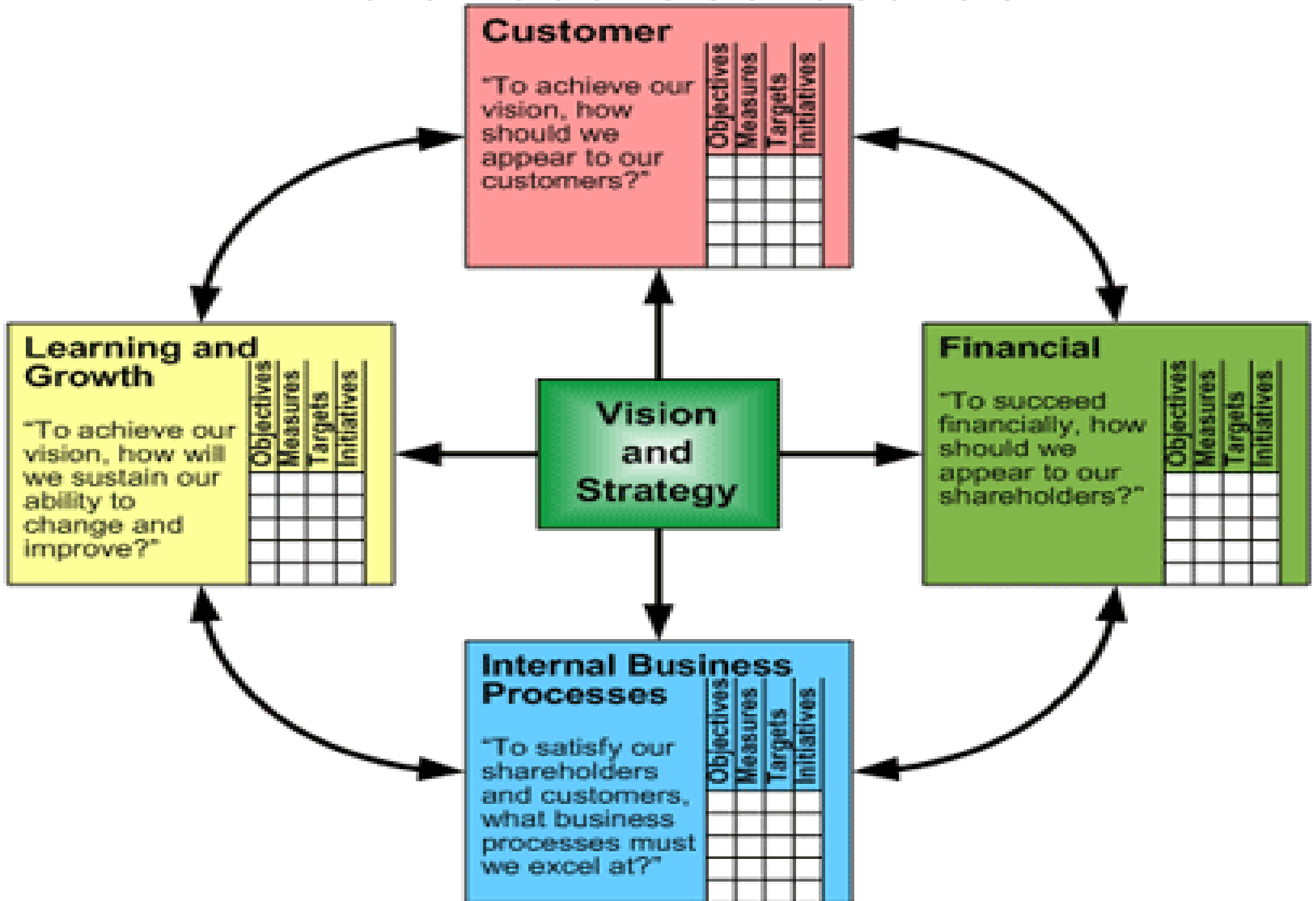
The sum is greater than the individual pieces



# Balanced Scorecards

- Focus on 4 key paradigms
  - Financial- Fiscal Measurements
  - Customer- Service Qualities
  - Operations- Operational Efficiency & Agility
  - Learning & Growth- Fostering Growth & Innovation
- Provides measurements based on key “customers” being serviced

# Balanced Scorecards



# Strategy Maps

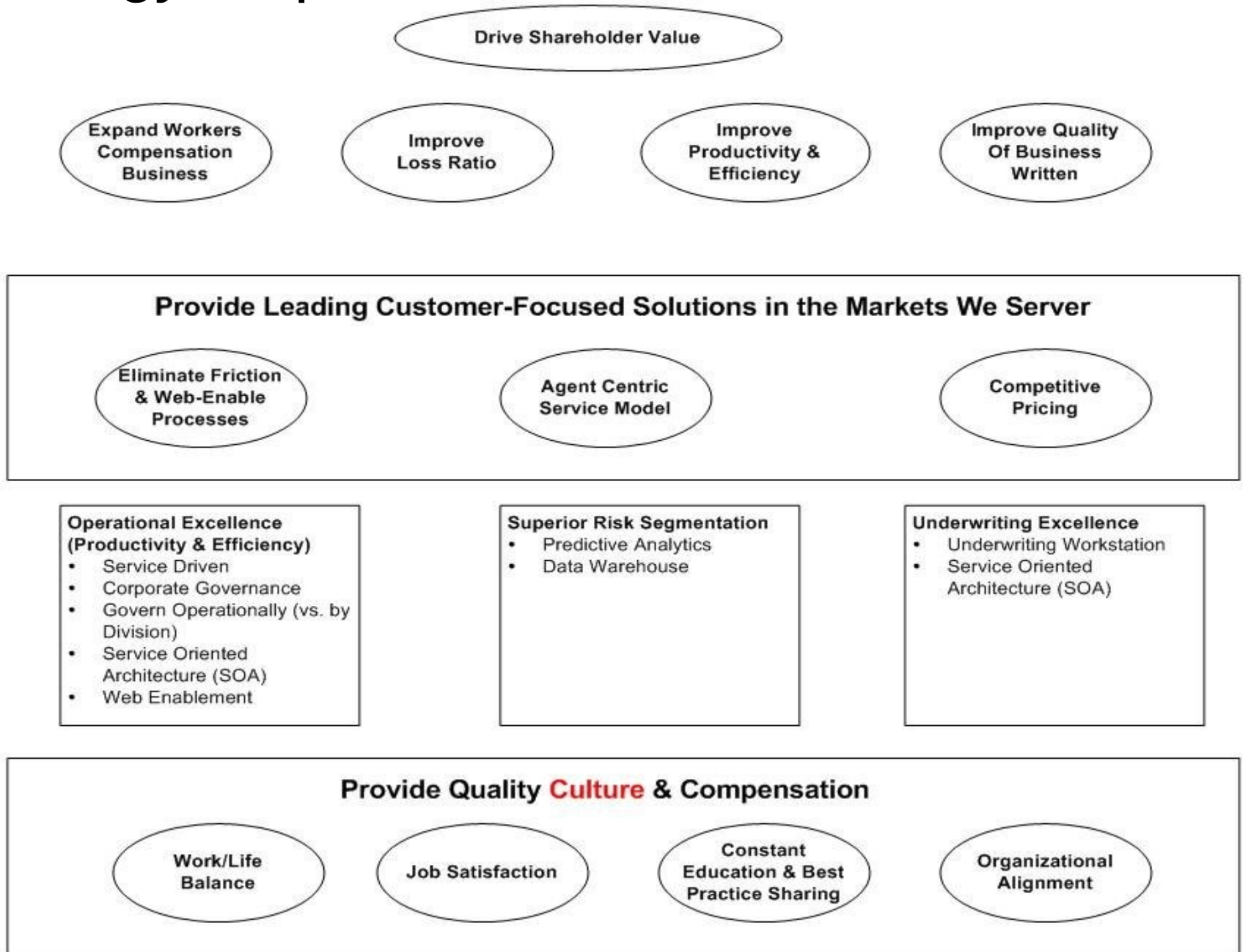
Describe the “To-Be” state graphically



- Facilitate collaboration
  - Minimize jargon
  - Collaborate

# Strategy Map

FINANCIAL  
CUSTOMER  
PROCESS  
PEOPLE






# Leading & Lagging Indicators

- Leading indicators
  - Sales Targets
  - # of site visitors expected this year
- Lagging indicators
  - \$ Closed Deals last month
  - Visitors last year
  - Amount a specific product has generated thus far

# KPIs & KGIs

- A Key Goal Indicator, representing the process goal, is a measure of "what" has to be accomplished. It is a measurable indicator of the process achieving its goals, often defined as a target to achieve.
  - Remain Profitable
  - Take over 15% market share in a territory
- By comparison, a Key Performance Indicator is a measure of "how well" the process is performing.
  - % of Bench time for engineers - "Riding the Pine"
  - # of opportunities in the pipeline

**F  
I  
N  
A  
N  
C  
I  
A  
L**

-  Manager of Information Security
-  Senior Security Engineer
-  Security Administrators

**Cost Effective Risk Management**

Roles:  
Vendor Consolidation  
Project Engagement \*  
Cost Justification

Measures:  
# of Vendors  
Cost & Residual Risk  
ALE (V)

**A  
G  
E  
N  
T  
S**

**Customer Friendly**

Roles:  
Chair Security Council  
Negotiate SLAs/OLAs\*  
Availability & Capacity Mgmt.  
Vendor Background Checks

Measures:  
Time-To-Close Requests  
# of SLA Deviations (A), (V)

**Diversified Access**

Roles:  
Quarterly Review of Access Solutions \*  
Simplify Existing Solutions

Measures:  
# Business Processes Optimized (A)

**Regulatory Compliance**

Roles:  
2 Gap Assessments per year\*  
Mapping Regs to Control Objectives

Measures:  
% PCI, HIPAA, & SB1386 Compliance  
% Identified Risks Addressed By Council  
Risk Response Trend by Category (RM)

**C  
U  
L  
T  
U  
R  
E**

**Account Management**

Roles:  
New Authentication/Authorization\*  
Engineering  
Operational Requests\*

Measures:  
# of New Requests  
# of New Users & Separations  
# of Requests By Department  
Time-To-Close Requests (R)

**Risk Management**

Roles:  
Semi-Annual Risk Analysis

Measures:  
# known physical risks  
# Risk-Based Exceptions (RM)

**Document & Communicate**

Roles:  
Policy, Procedure, & Standards Mgmt\*  
Yearly Security Training

Measures:  
% of Policies, Procedures, & Stds. deployed  
# of Pending Requests (A)

**Security Controls**

Roles:  
Controls Management

Measures:  
# Risks w/o Controls  
# Uncompleted Requests  
# Control Violations Identified (RM)

**Service Catalog**

Roles:  
Publish & Manage Services\*

Measures:  
# of Pending Requests  
# of Requests Per Service  
# of Requests Not In Catalog (A) (V)

**Vulnerability & Patch Management**

Roles:  
Vulnerability Management  
RFC Submissions  
Auditing Patch Levels  
E-Commerce Testing\*

Measures:  
# High/Med/Low Int. & Ext. Vulnerabilities  
# of Patches Required  
# RFCs Complete / Incomplete  
# New External Facing Applications / # Tested (RM)

**Security Event Management**

Roles:  
Countermeasure Management  
Incident Response\*

Measures:  
# of incidents  
# of validated issues by category (RM)

**Today  
Tomorrow  
Together**

**Training & Career Development**

Roles:  
Identify Curriculum  
Manage/Mentor Career Paths

Measures:  
# Certifications Achieved  
% of career paths tracking (A) (R)

- \* = Services
- (A) Alignment with Business Strategy
- (P) Performance Measurement
- (R) Resource Management
- (RM) Risk Management
- (V) Value Delivery

# Prudent Management is not just for the enterprise anymore

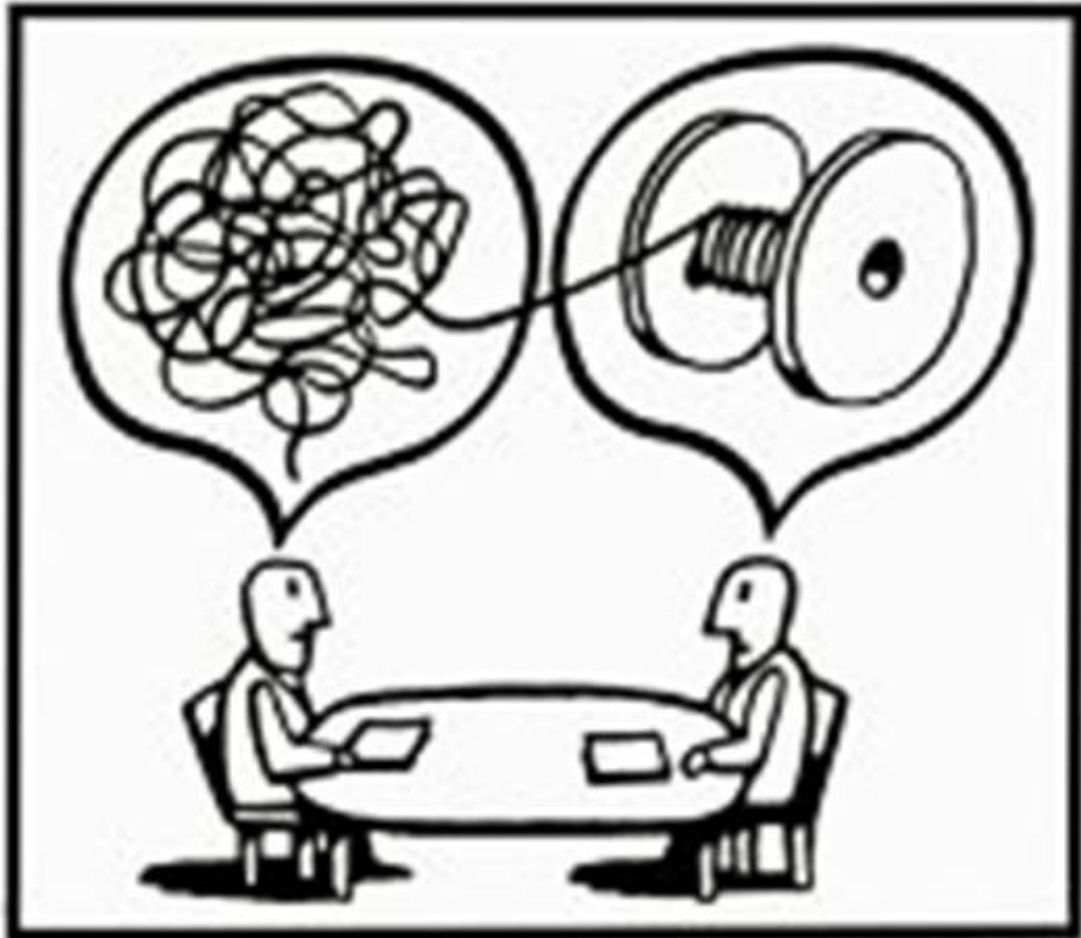
- Governance has been slowly adopted in the SMB space
  - Perceived as an “enterprise play”
  - ROI/CBA/NPV communication muddled with jargon

**Talk to your audience- don't belabor acronyms and frameworks.**

**Focus on sound stewardship principals.**

# References

- Privacy Violations- [www.privacyrights.org](http://www.privacyrights.org)
- COBIT - [www.isaca.org/cobit](http://www.isaca.org/cobit)
- VAL IT - [www.isaca.org/valit](http://www.isaca.org/valit)
- Strategy Maps -  
[http://www.valuebasedmanagement.net/methods\\_strategy\\_maps\\_strategic\\_communication.html](http://www.valuebasedmanagement.net/methods_strategy_maps_strategic_communication.html)
- BSC - <http://www.balancedscorecard.org/>
- Lean Six-Sigma - [www.qimacros.com](http://www.qimacros.com)
- Harvard Business Review



# Questions?



Jeromie Jackson- CISM, CISSP  
Security Solutions Architect  
Technology Integration Group (TIG)  
Jeromie.Jackson@Tig.com  
858-205-3645- BB  
619-368-7353-cell