IT Optimization & Risk Management

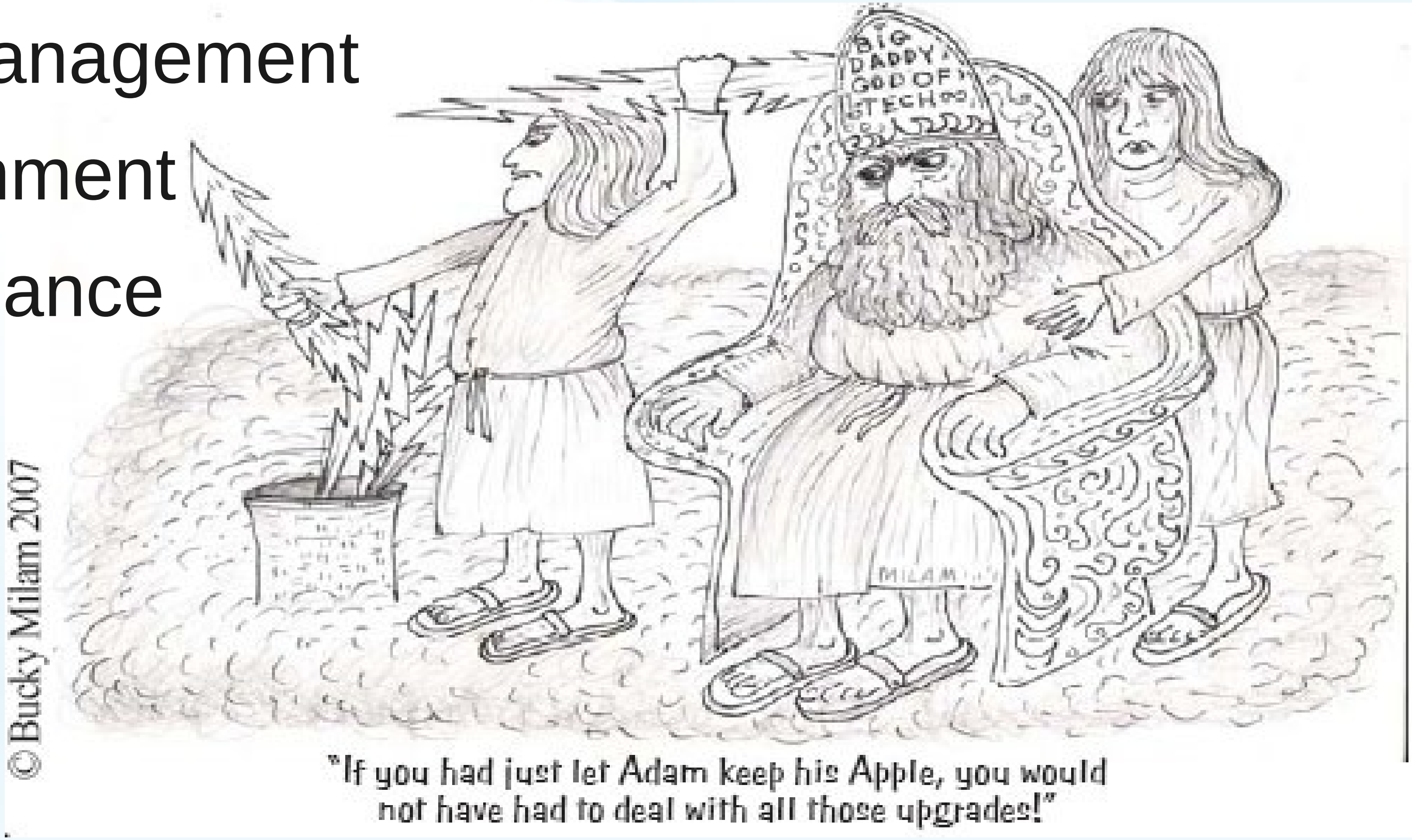
Jeromie Jackson – CISSP, CISM
Jeromie.Jackson@Tig.com / Jeromie@comsecinc.com
619-368-7353

About Me

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

Board Concerns

- Profitability
- Satisfying Regulations & Passing Audit
- Risk Management
- IT Alignment
- Governance



"If you had just let Adam keep his Apple, you would not have had to deal with all those upgrades!"

Down Economy causing executives to focus on profitability

- 3 ways to improve profitability
  - Increase top-line sales
  - Reduce COGS
  - Optimize Operations

Regulations

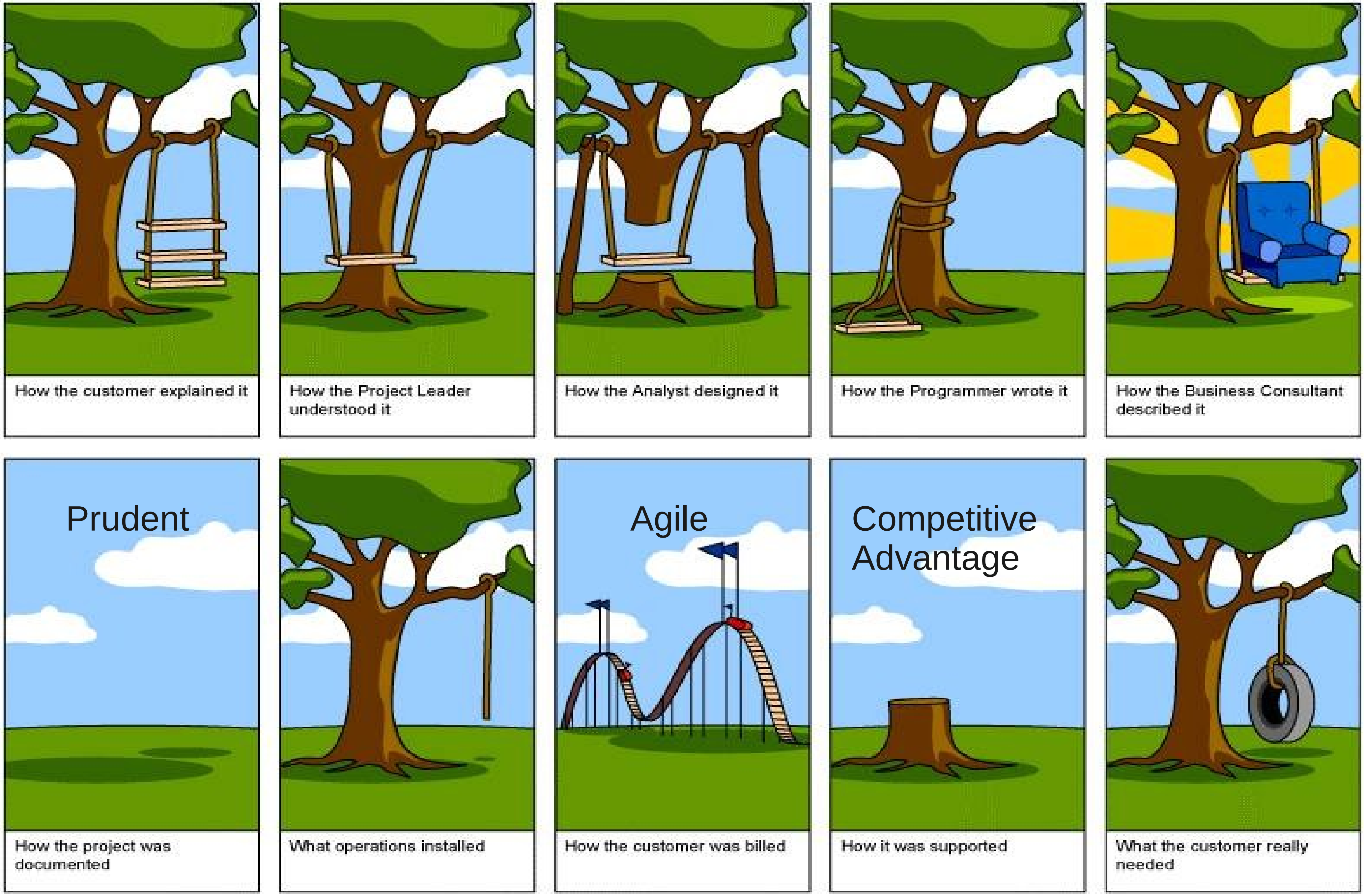
NYSE
Sarbanes-Oxley
Audit and Risk Management
FERC
IT Staff Management
HIPAA
CobIT Control Obj
PCAOB
PCI DSS
ISO
NASD
Technical Security
DOD
OCG ITIL
Basel II
NIST
400+ regulations, standards, & guidelines
Across 38 countries
Over 10,000 overlapping controls
One UCF

- Overlap
- Minimal benefit
- Increasing complexity
- Resource intensive
- Divert focus on maturing risk management

Security Risks & Exposures are Growing

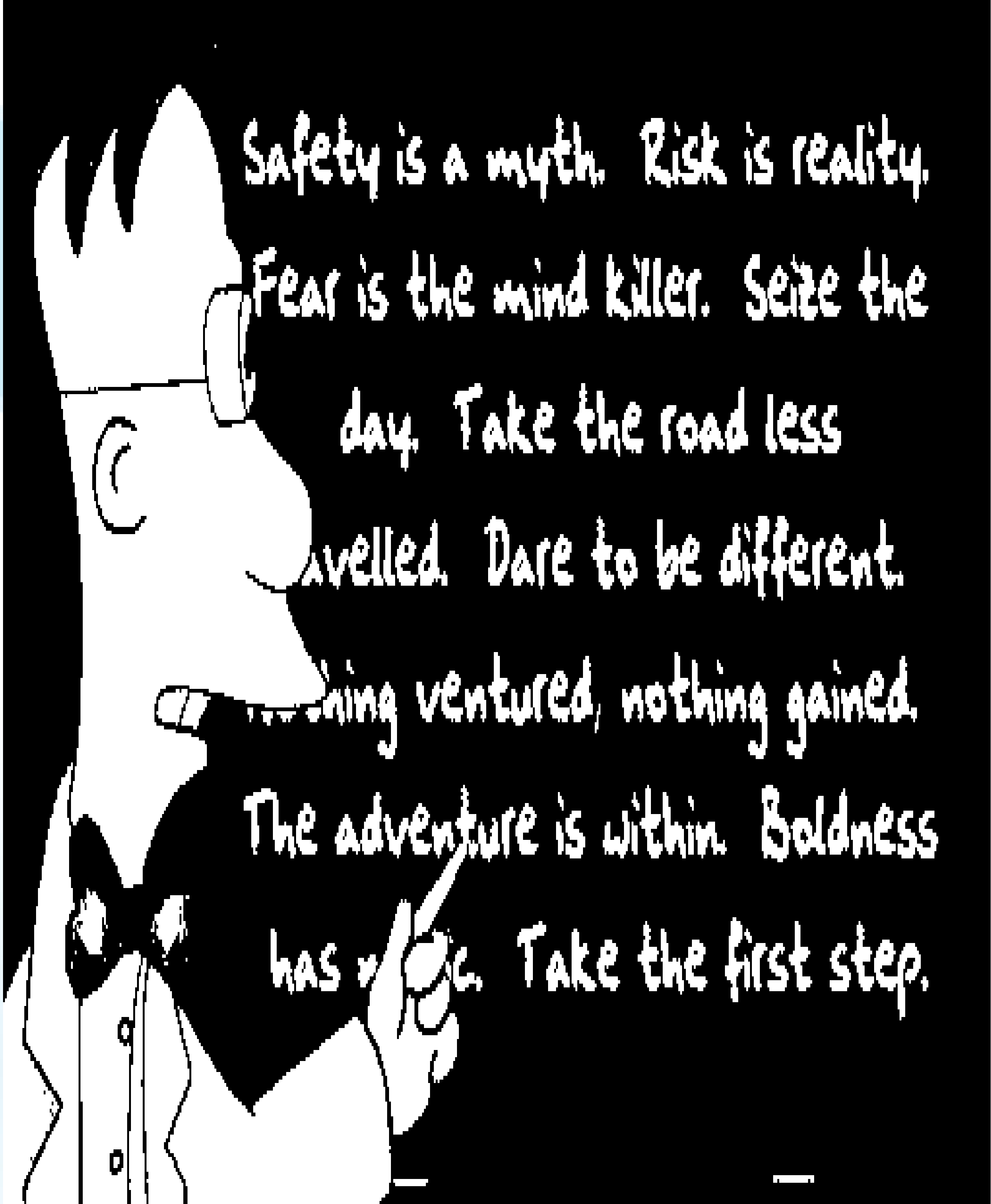
- More than 35 million data records were breached in 2008 in the United States
  -Theft Resource Center
- Jan 20, 2009- Heartland Payment Systems- *100 Million Transactions Per Month!*
  http://www.2008breach.com/
- 252,276,206 records with personal information since January 1995
  - www.privacyrights.org

IT & Business Alignment- Are we communicating?


How the customer explained it
How the Project Leader understood it
How the Analyst designed it
How the Programmer wrote it
How the Business Consultant described it
Prudent
How the project was documented
What operations installed
Agile
How the customer was billed
Competitive Advantage
How it was supported
What the customer really needed

Implications

- IT is meant to serve the business
- IT must be aligned with business goals
- IT is costly and requires prudent management

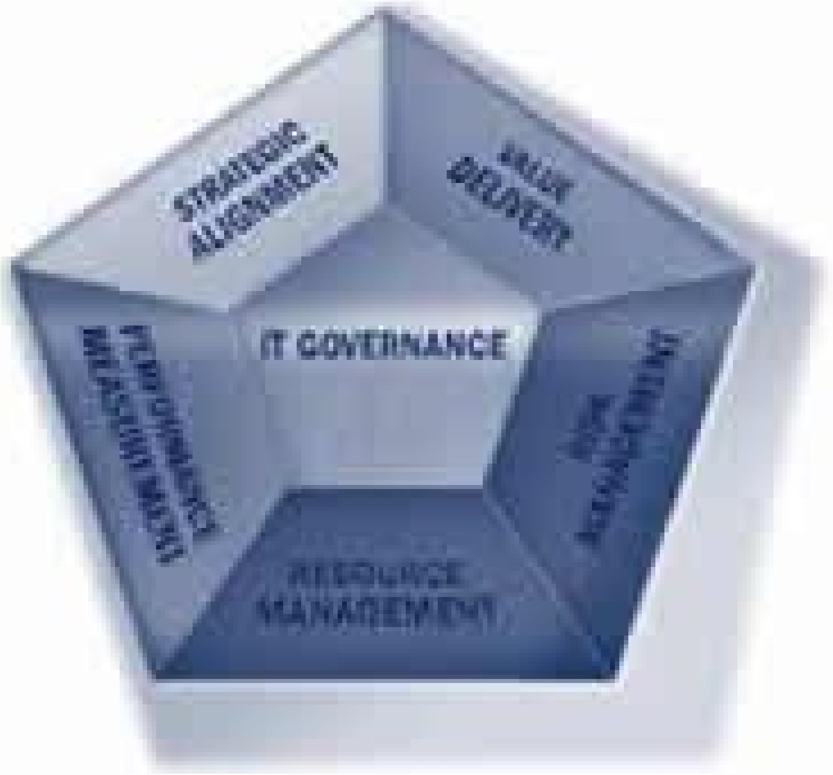

Safety is a myth. Risk is reality.
Fear is the mind killer. Seize the
day. Take the road less
velled. Dare to be different.
hing ventured, nothing gained.
The adventure is within. Boldness
has c. Take the first step.

Become Proactive

- Instill best-practice governance
- Utilize a risk-management portfolio to guide remediation
- Consolidate Regulations

5 Facets of Governance

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



Improve Risk Management

- Risk Management Process
  - Identify critical assets
  - Define containers
  - Identify risks & threats
  - Quantify or qualify risks
- Prioritize Remediation Efforts

Risk Management Frameworks & Functions

- Frameworks
  - NIST (SP800-30)
  - Octave
  - Octave Allegro
  - Factor Analysis for Information Risk (FAIR)
- Primary Functions

Create Value	Account for People, Process, and Technology
Integral Organizational Process	Continual
Systematic	Focused on Continual Improvement

Regulatory Convergence

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

Optimize IT

- Bridge the gap between control requirements, technical issues, and business risk
- Use a portfolio approach to risk management
- Manage by measurement
- Enable your organization to reap maximum benefit from technology investments

Questions?

ISACA®
Serving IT Governance Professionals
San Diego Chapter

Jeromie Jackson- CISSP, CISM
Jeromie@ComSecInc.com /
Jeromie.Jackson@TIG.COM
619-368-7353-direct
http://www.linkedin.com/in/securityassessment