DIGITAL SECURITY true

ICSJWG 2010 Spring Conference

San Antonio, Texas

April 6-8, 2010

Beyond Regulatory Compliance toward a Comprehensive Security Program

True Digital Security

Jerald Dawkins, Ph.D.

Agenda

- Motivation
- What is a security program
- Maturity of security programs (where are you)
- Strategies for achieving regulatory compliance
- Architecture of a security program
- Five steps to achieve a comprehensive security program

Motivation

- Findings
  - Cyber security for ICS is unclear and requires consolidation and development
  - While IT cyber security can provide a foundation, ICS operations have distinct difference due to environment and requirements
  - Current efforts focus on technical standards rather than on delivering a solution
- Recommendations
  - Establish a formal top-down plan as part of overall operations governance
  - Establish cyber security coverage in ICS operations with well defined roles and required skill sets
  - Prioritize critical gaps in cyber security based on compliance mandates (e.g. CIP) and IT security process refinements

What is a Security Program

- Firewall
- Active directory
  - Username and passwords
- Anti-virus protection
- VPNs
- The end. Questions?

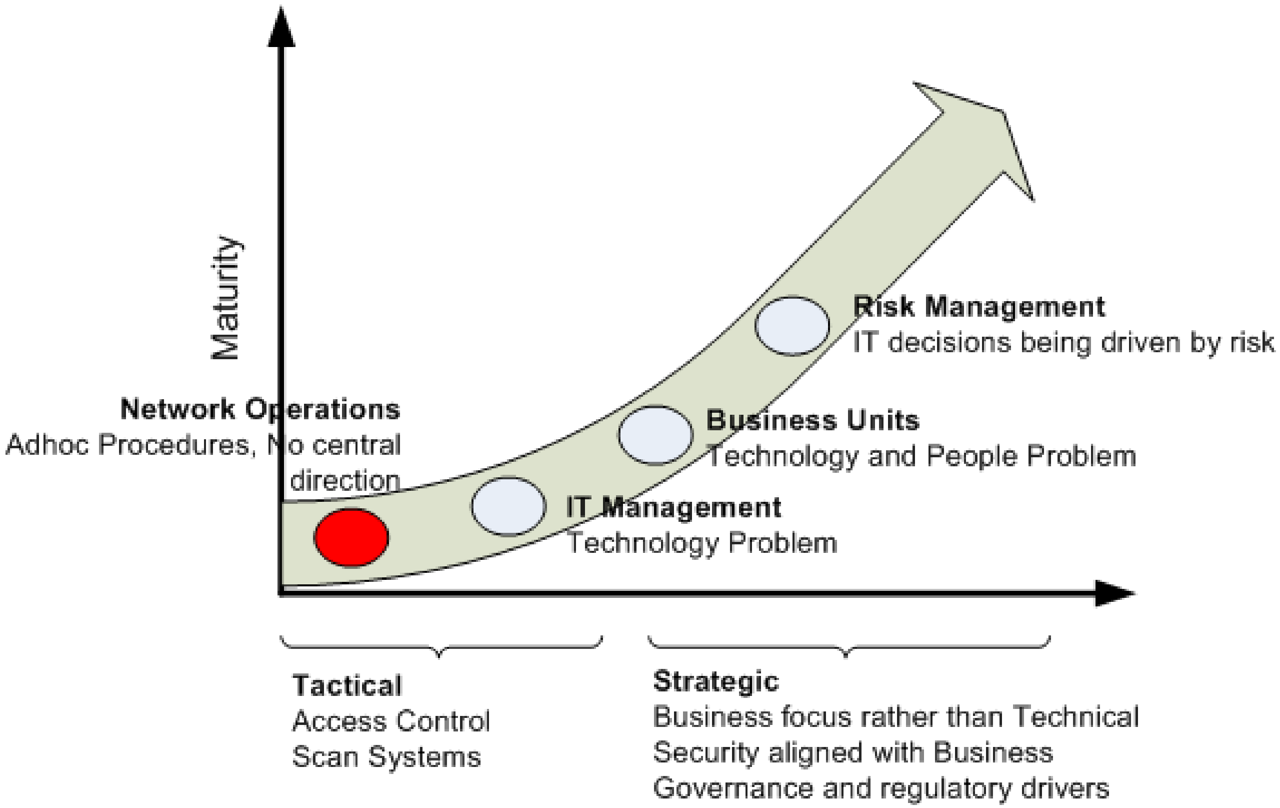
What is a Security Program

- Daily operational challenges
  - Employment hiring, termination, and change
  - System planning and acceptance, change control
  - Staying apprised of new threats to technology
  - Monitoring technology
  - Conducting regular security testing
  - Establishing compensating\mitigating controls
- The Reality
  - Timeframe to establish and maintain
  - It’s a people and process problem, too
  - Technical challenges exists
  - Point in time assessment versus continuous security program

Where Are You?

- Proactive or reactive?
- Technology, business or compliance focus?
- IT Governance and Compliance initiatives identified?
  - NERC, PCI
  - ITIL, NIST, NSA
  - HIPAA, HITECH
- Have your policies and procedures been adopted?
- Are you reporting\monitoring your security initiatives?

Tactical versus Strategic



Maturity

Network Operations
Adhoc Procedures, No central direction

IT Management
Technology Problem

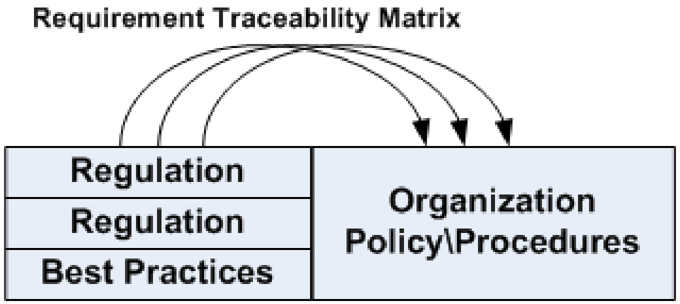
Business Units
Technology and People Problem

Risk Management
IT decisions being driven by risk

Tactical
Access Control
Scan Systems

Strategic
Business focus rather than Technical
Security aligned with Business
Governance and regulatory drivers

Approaches to Achieve Compliance



Requirement Traceability Matrix

Regulation	Organization Policy\Procedures
Regulation	
Best Practices	

Compliance Driven

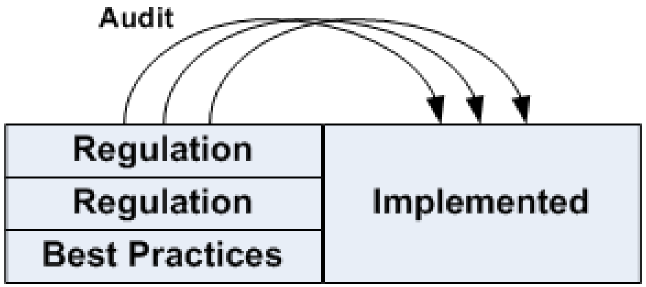
- Compliance drives policy\procedural development
- Implementation is difficult, expensive and “compliance-date” driven
- Disconnect between actual processes and documentation

Result: **FAIL**

Technology Driven

- Compliance drives “toolkit” purchasing
- Implementation is “service-driven”
- Results in:
  - Strained resources
  - Band-aid repairs
  - Increased spending

Result: **FAIL**



Audit

Regulation	Implemented
Regulation	
Best Practices	

Implementation Strategy

Cyber Security Policy

Electronic Security Perimeter

Change Control Management

Electronic Access Control

Cyber Vulnerability Assessment

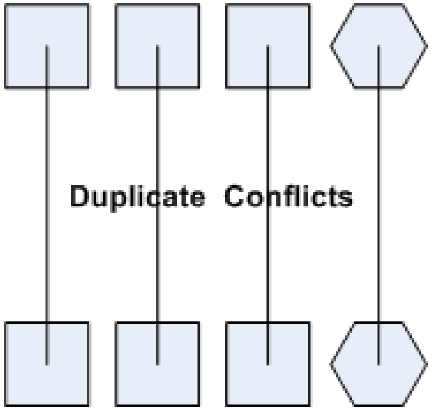
Information Security Policy

Firewall Configuration Policy

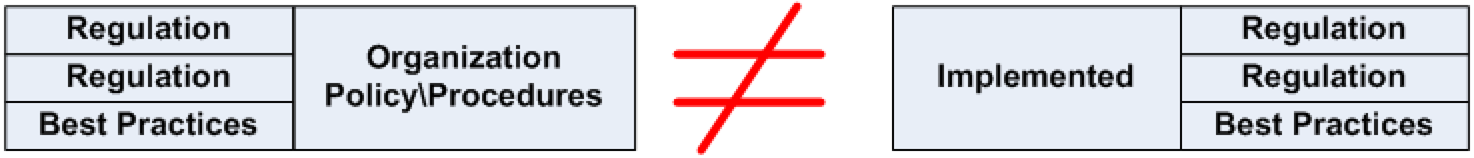
Secure Software Development

Intrusion Detection

Vendor Management

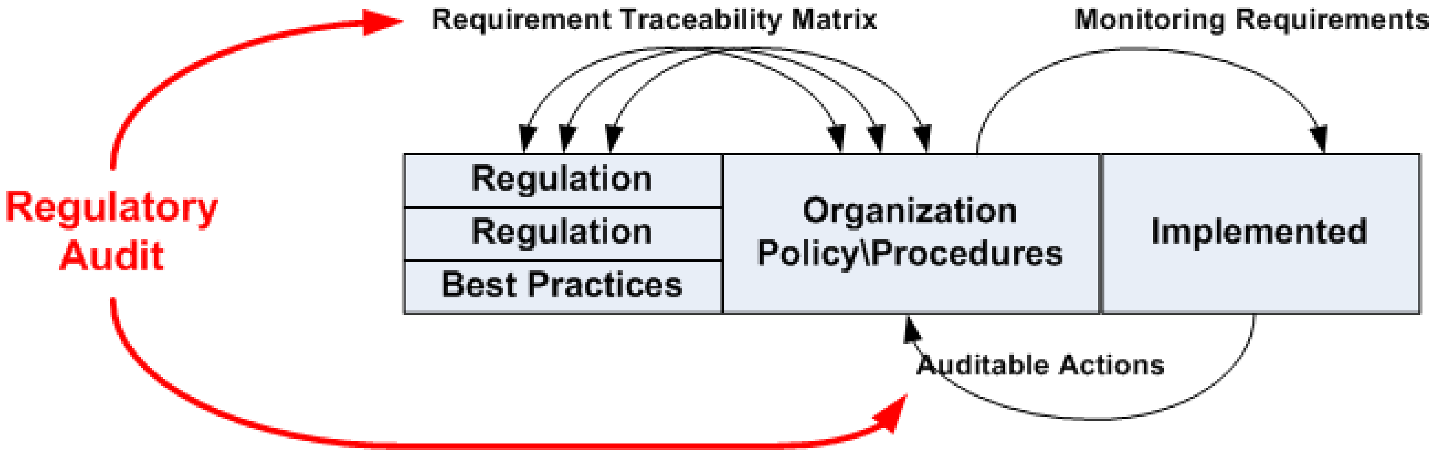


Misaligned Compliance Objectives



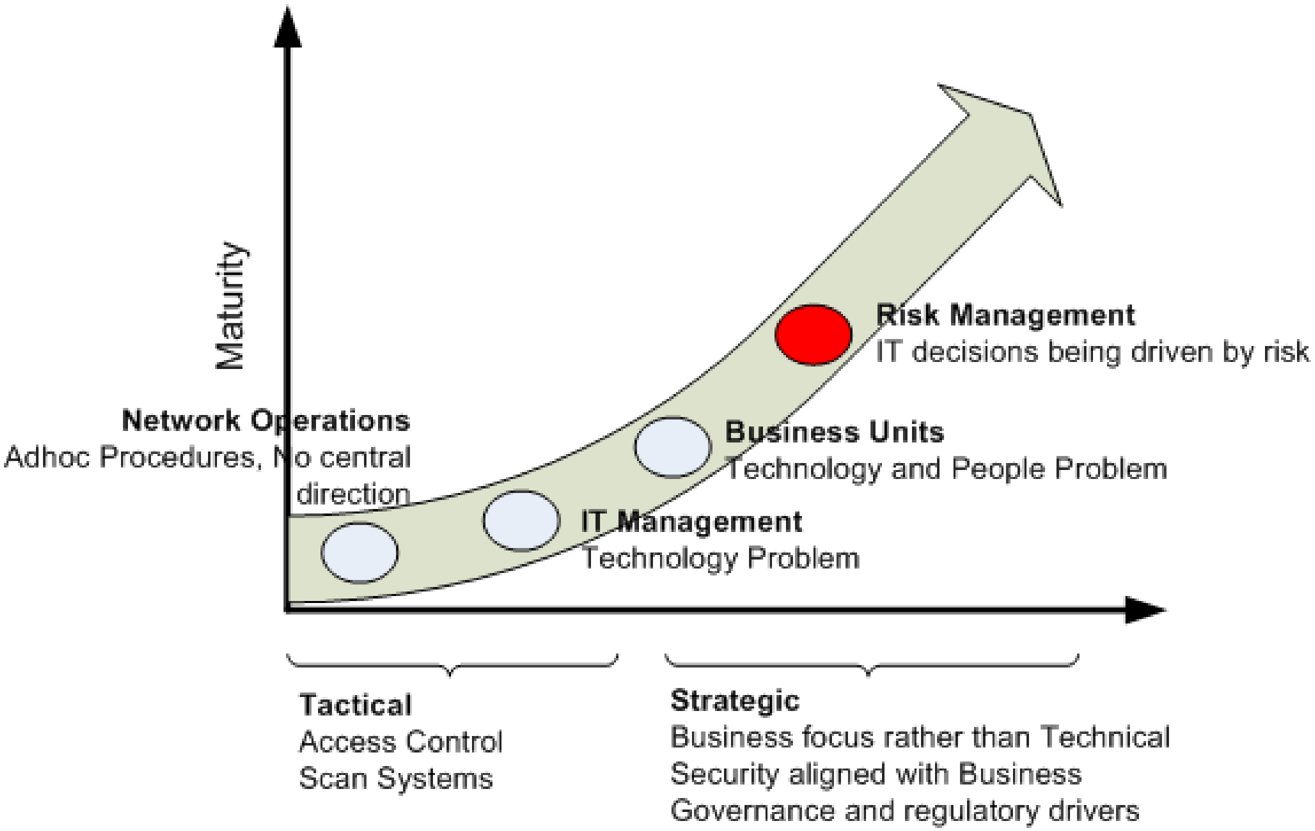
- Internal and external audits are time consuming
  - Internal resources to answer auditor questions
  - Producing action items to satisfy audit requests
- Business drivers ≠ technology
- Managing a security program is:
  - Confusing (regulation)
  - Time consuming (multiple parts)
  - A challenge to monitor (cross-department involvement)
  - Often overlooked (always something more important, insufficient ownership)

Aligned Security Program

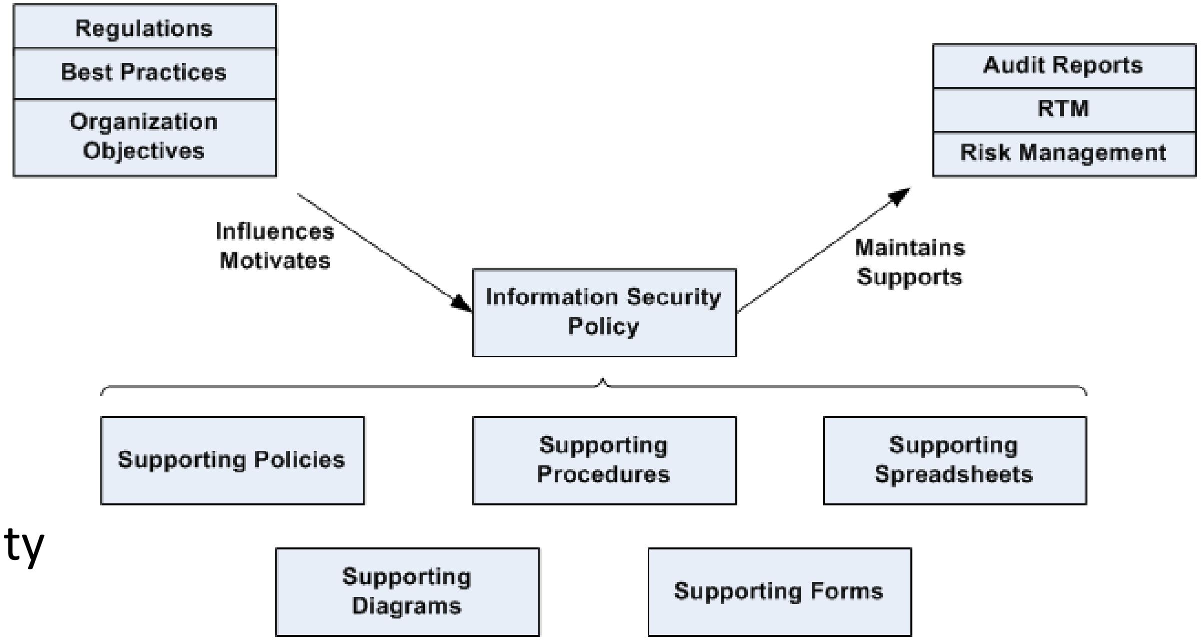


- Technology aligns with policies and procedures
- Policies support procedures
- Procedures are designed to enable monitoring
  - Repeatable, Changeable, Auditable
- Regulations are map-able, not drivers
- Mature remediation process
- Annual updates and tweaking

Strategic Security Program

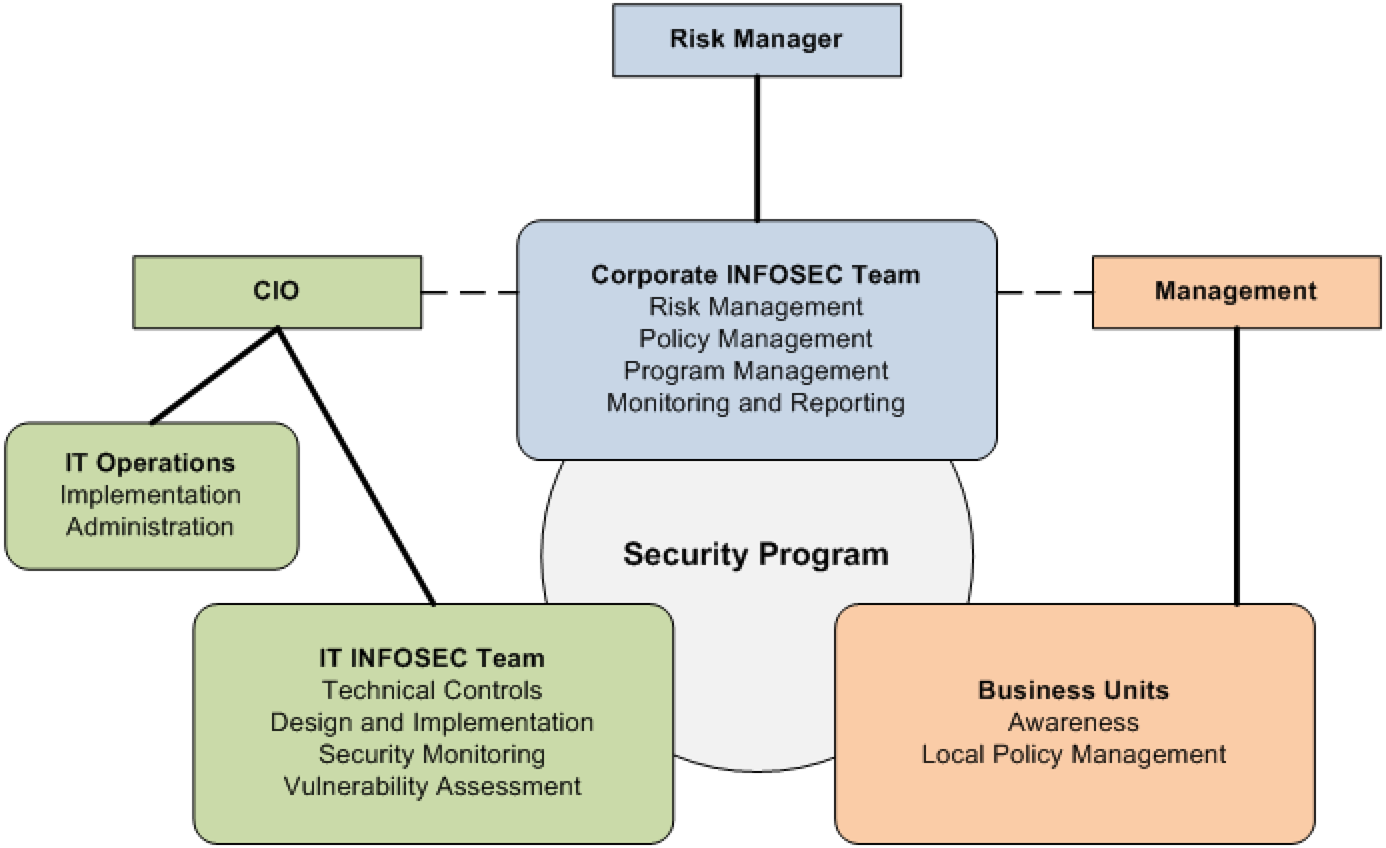

Maturity
Network Operations
Adhoc Procedures, No central direction
IT Management
Technology Problem
Business Units
Technology and People Problem
Risk Management
IT decisions being driven by risk
Tactical
Access Control
Scan Systems
Strategic
Business focus rather than Technical
Security aligned with Business
Governance and regulatory drivers

Security Program Structure



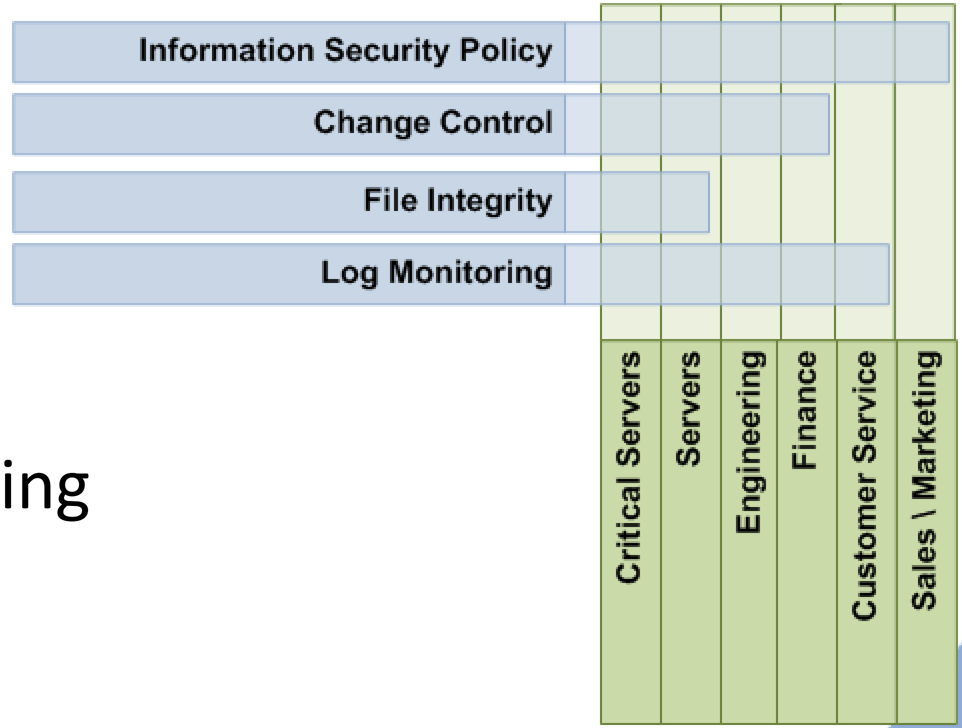
- Accountability
- Governance
- Technology Balance
- Risk-Based
- Reporting
- Business Alignment

Security Program Management



Steps to Security Program

1. Understand the Environment
2. Determine Scope
3. Controls (Gap Analysis)
4. Project Planning
5. Implementation
6. Execution and Monitoring



Lessons Learned

- Business decision makers fail to recognize the value of security and its impact on their business goals
- Mature information security programs typically spend less than comparable organizations
- Accountability owned by CIOs and CSO instead of business lines
- Balancing security and operations
- Formalizations improves process maturity, improving effectiveness and efficiency
- Staff resistance constitutes one of the bigger challenges

Questions \ Comments

Jerald Dawkins
jdawkins@truedigitalsecurity.com
918-770-7700 x101