



Identity Theft & Database Security

Best Practices to Securing Client Data

John Verry

Principal Enterprise Security Consultant

Pivot Point Security

September 21, 2005

Community Bank Association of New York

Syracuse, NY

About this Presentation

- Will not be “Death by Power Point”
- Dialogue (not Monologue)
- Will discuss Database Security as a business issue (not a technical issue)
- Goal is to introduce key concepts and get the session to be interactive

Shaping the Presentation

- Understand the audience
 - Roles
 - Reason/goal for being at session
- About the Presenter
 - Provides context for viewpoints

A Sad State of Affairs

- Bank of America - 1,200,000 records (Federal Employees, even US Senators!)
- Lexis Nexis - 310,000 records
- Ralph Lauren - 180,000 records
- Choice Point - 150,000 records
- DSW Shoe Warehouse - 145,000 records (750 confirmed fraud cases)
- Las Vegas DMV - 9,000 records



What Happened?

- Bank of America - “Lost” data tapes; possibly stolen by commercial air baggage handlers
- Lexis Nexis - Social Engineering (fraud), unspecified breakdown of internal customer credentialing process
- Ralph Lauren - Not specified yet, but associated with a “US-based retailer”, according to MasterCard
- Choice Point - Social Engineer & Fraud; via forged documents such as business licenses, thieves became a Choice Point “customer” and gained access to customer data
- DSW Shoe Warehouse - “Traditional” technology hack; details not disclosed
- Las Vegas DMV - Physical break in/theft of computer containing 3 months worth of drivers license data (SS #, photo, signatures, names, age, etc.)

Personal Identity Theft Experience

- Four Different Examples of Identity theft
 - Hack of Governmental HR Database
 - Hack of Confidential Patient Health Information from Health Care Provider
 - Hack of Credit Card Data from NPO
 - Hack of Client Data from International Bank
- Four Distinctly Different “causes”
- Four Distinctly Different Solutions

Identity Theft via Control Environment

- Large Governmental Agency looking to deploy People Soft HR to 200K+ Employees
- Application and network hosting application were highly secure
- LAN administering was very secure – except for a single old NT4 system
- Password Policy could not be enforced – weak Admin PW lead to PW crack of LAN Admin PW
- Non-optimal AV missed planted keystroke logger
- Garnered root access on Oracle & People Soft with personal info on 400K employees including SSN's
- Solution: Risk Assessment, Compliance Monitoring of PW, Control Objectives updated to address spyware & loggers

Identity Theft via Network Hack

- Large Health Care provider looking for HIPAA validation
- Application & systems hosting application were highly secure
- Cisco switches had older IOS software
- VoIP Telephones running older software
- “ARP Spoofed” the switch to see a copy of all network traffic including clear text passwords
- Recorded privileged conversations between clients, doctors and Health Care Provider
- Gained access to full client health data
- Solution: Network Configuration Management, Risk Assessment modifications

Identity Theft via Application Hack

- NPO had rolled out new donor web portal
- System and Network were highly secure
- App was subject to SQL Injection (Select *) & Forceful browsing to Administrative Interface
- Retrieved 1,000 + user names, donation history, and credit card data
- Solution: Security Testing Policy, Data Classification Policy, Application Firewall

Identity Theft via Database Hack

- International Bank had concerns re hosted Fund Transaction system
- SQL Server back end running vulnerable services
- Used ISQL vulnerability to create Admin User on System
- Elevated access to DB Admin
- Garnered access to hundreds of high value clients (\$500M)
- Solution: Database Monitoring Policy, Data Classification and Data Ownership Policy updates, Database Intrusion Protection Software

Good News – Identity Theft is Usually the Breakdown of Multiple Controls

- Identity Theft is usually the result of a breakdown of multiple levels of the control environment
 - Administrative Controls (Executive Management – think policies & strategic planning)
 - Operational Controls (Business/IT Management - think procedures & tactical planning)
 - Technical Controls (IT Personnel – think devices/systems and their administration)
- Holistic View Necessary
- Your client data lives inside your Information Systems Control Environment
- How do you (the CEO) take accountability for Data Security ?
 - Information Technology Governance

IT Governance for the CEO?

- Start at the Core
 - Formally communicate your **Business Strategy** & Control objectives (Do they *really* know where you are going?)
 - Embrace **Risk Assessment** at a Business & Information Technology level (Do they *really* know what the risks are, what the ROI on each risk mitigation is, and what is an acceptable level of risk?)
 - Ensure **Regulatory Compliance** is considered and communicated (Do they *really* take the time to understand the implications of HIPAA, SOX, SB-1386?)
 - Validate and enforce your current **Information Technology Control Environment** (Are personnel *really* aware of key control elements?)
 - Enforce and measure against your **Information Technology Strategic Plan** (Does the plan align with your organizational objectives and are they *really* leveraging it?)
- Force discussion with IT to a business level
- Find a trusted advisor to keep you up to speed on emerging issues

Risk Assessment is a key

- First & Foremost – Understand the Risks
 - Conduct a Risk Analysis
 - Allows you to prioritize risks
 - Allows you to quantify risks (\$'s)
 - Allows you to validate ROI (\$50 Horses)
 - Ultimately results in a Roadmap
- Second Understand Your Options
 - A Strong Technical Control may provide short term compensation for greater sins
 - There is almost always more than one way to skin a cat
 - Keep your conversations on Information Technology at a Business Level
 - What Risk (to a strategic or control objective) does this proposed control address?
 - How does this help me achieve this control or strategic objective
 - What is the residual risk?
 - How do we ensure compliance with the new controls ?
 - What upstream and/or downstream controls are necessary to support the proposed control?
 - What training, education, documentation changes are necessary to support the proposed control?
- Monitor Effectiveness of the controls
 - ROI Achieved
 - Control Objective achieved
 - Adjust as necessary (continual improvement)
- Iterate

Emerging Technical Controls for Identity Theft

- Application Firewalls (e.g., F5)
 - Front ends Web Applications and blocks most malicious attacks
 - SQL Injection
 - Cross Site Scripting
 - Command Injection
 - Buffer Overflows
 - Can be use for problematic application (vendor provided, under development, short term protection)
 - BCan be used long term on critical applications (belt & suspenders)
 - Zero Day Attack Protection
 - Coding error Protection
- Network Configuration Management (e.g., Alter Point)
 - Enforces Policy and Procedure for Network Devices
 - In a WELL run organization 1% of Network devices will have a serious flaw
 - Blank or weak password
 - Clear Text Authentication
 - Vulnerable services enabled
 - Outdated Software
 - Configuration Mistakes

Emerging Technical Controls for Identity Theft

- Database Intrusion Protection (e.g., Application Security Inc.)
 - Provides ongoing monitoring of Database for vulnerabilities and access falling outside policy
 - Identifies Vulnerabilities
 - Actively Prevents Attacks
 - Privilege Escalation
 - Web Application Attacks
 - Operating System Access
 - e use for problematic application (vendor provided, under development, short term protection)



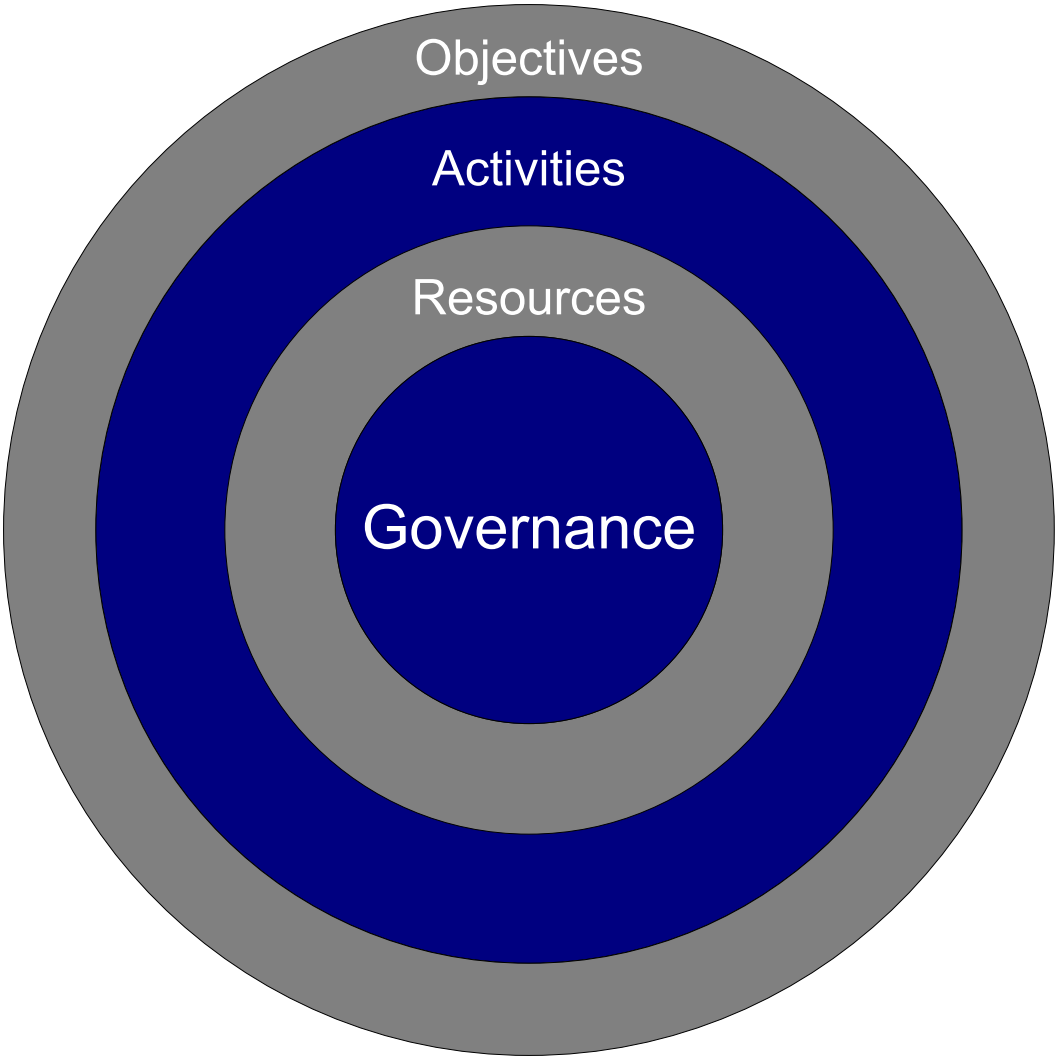
Wrap Up

- Q & A
 - jverry@pvtpt.com / (732) 267-6324

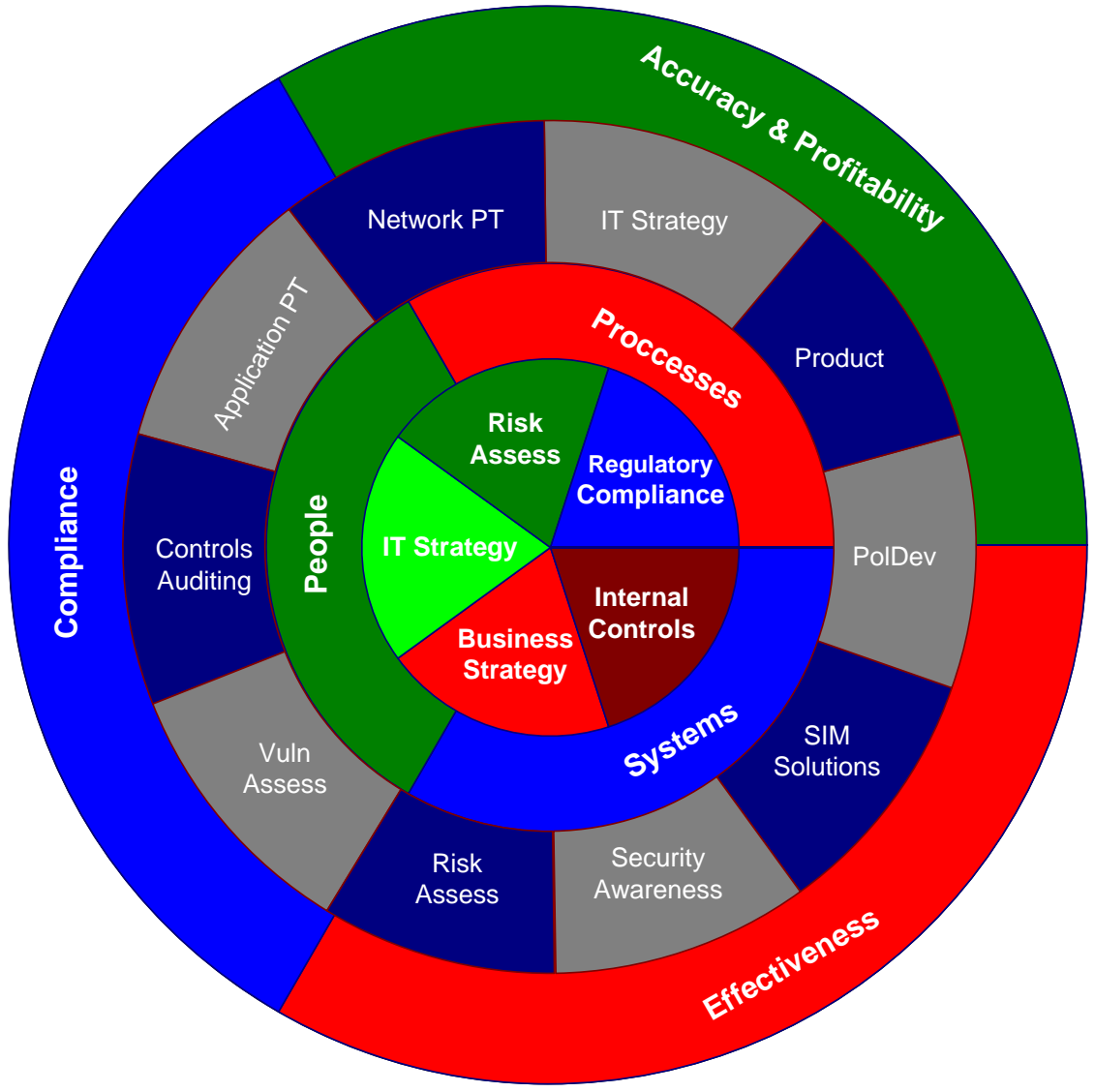
Take your own temperature - Do these Key Controls exist?

- If you are not aware of these key controls then you may be at higher than acceptable risk:
 - Systems Development Lifecycle Methodology (SDLC) -- a logical structured approach to System Acquisition/Development, Deployment, & Maintenance
 - Data/System Ownership
 - Data Classification
 - System Interfaces
 - Segregation of Duty
 - Passwords (sharing, strength)
 - System Audit (logging)
 - Independent Review & Validation (Annual External audit is not sufficient)
 - Technology Oversight Committee (functional vs. titular)

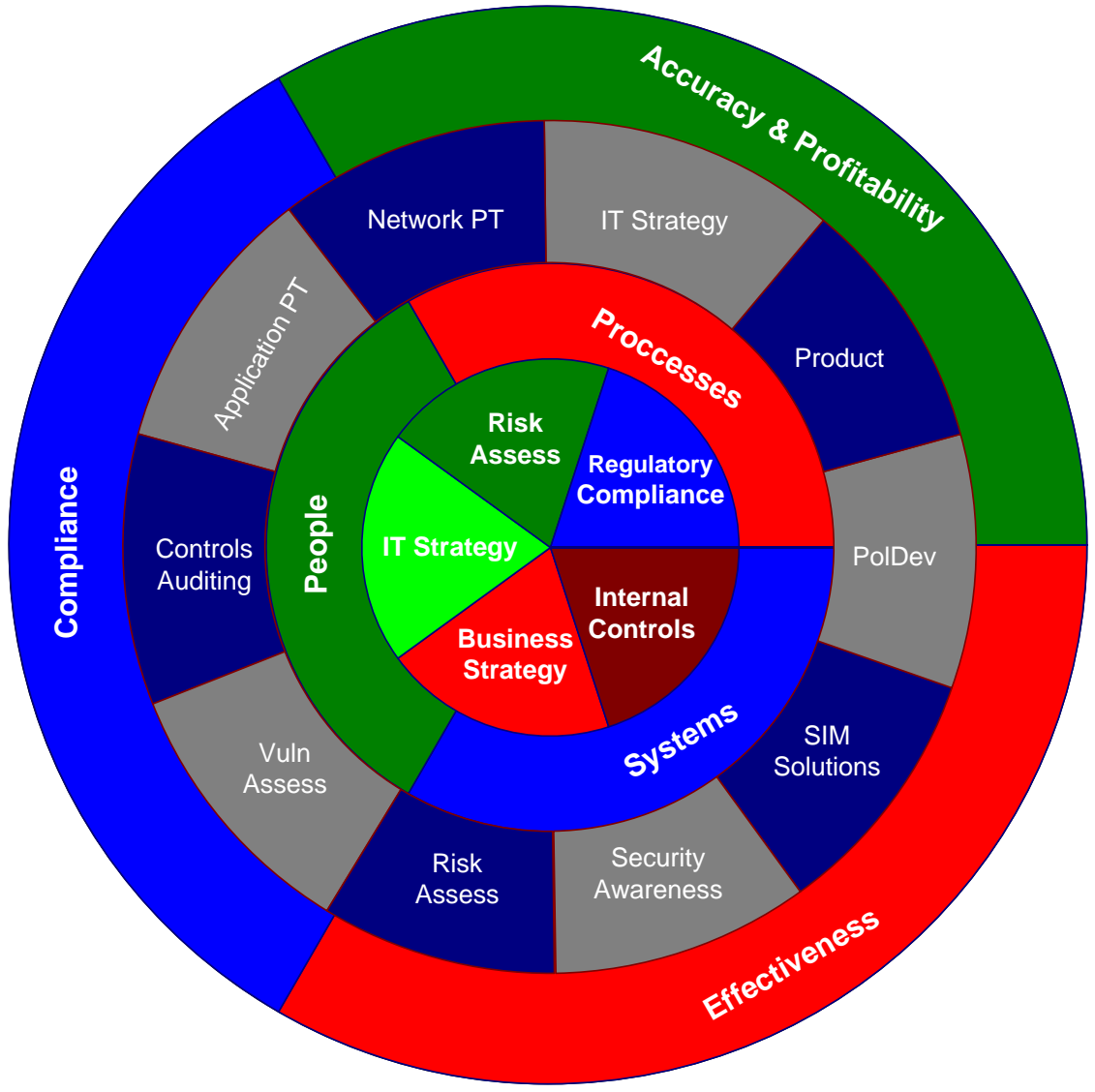
Audit Based InfoSec (ABIS)



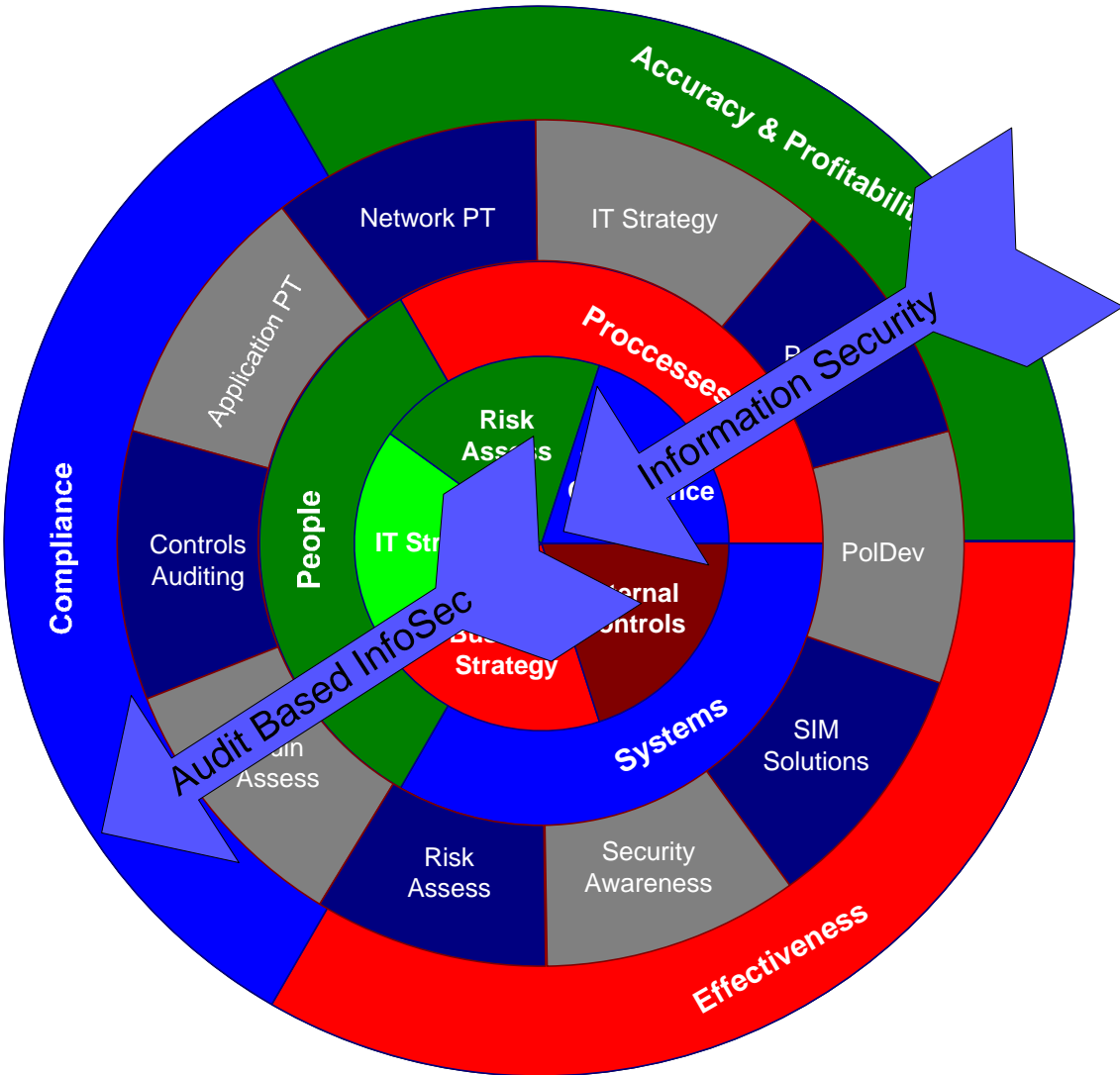
Audit Based IS - Detail



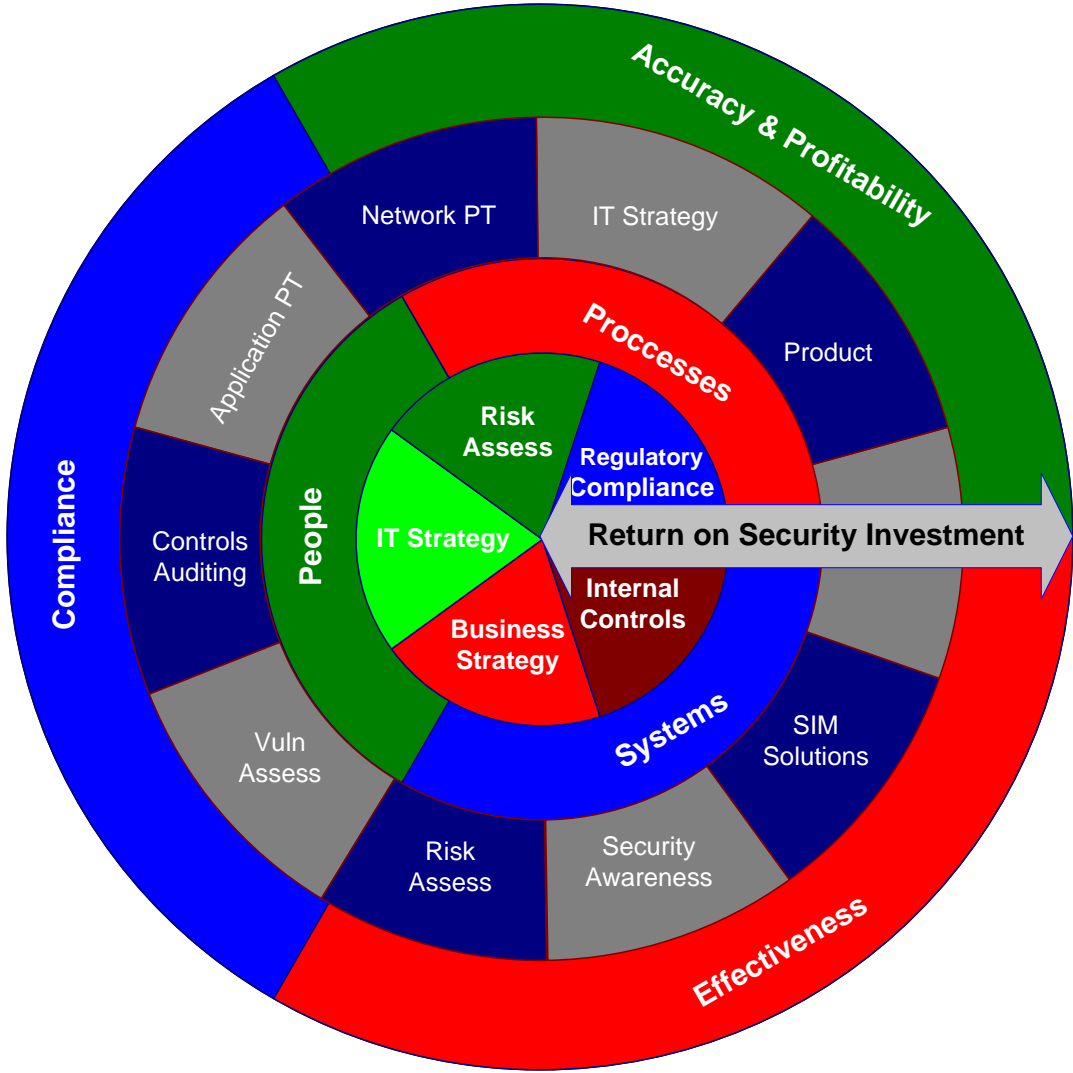
Audit Based IS - Detail



Audit Based IS vs. IS



Audit Based IS & ROSI



Impact for IT Management

- Defense in Depth has changed:
 - Previous Model was largely premised on product layers
 - Router ACL, Perimeter Firewall, Desktop IPS
 - New Model is largely premised on “Control” Layers
 - Managerial Control, Operational Control, Technical Control
 - Policy, Procedure, Standard
 - The key is to work from the Core
 - (Risk + Regulatory Compliance + Strategic Business Objectives + IT Strategy) Drive Control Objectives
 - Control Objectives Drive Policy
 - Policy Drives Procedure
 - Procedure Drives Standards

Impact for IT Management

- More emphasis on Detect Controls
 - Monitoring & Compliance Tools are the rage
 - Security Event Management gets a new coat of paint (and is salvaged from the IDS “stigma”)
 - Awareness, Forensics, and Compliance from a single data source
- More emphasis on “non-technical” Prevent Controls
 - Security Awareness Training
 - Risk Assessment
- More emphasis on Managerial and Operational Controls
 - SDLC is no longer a four letter word
 - Technology Oversight Committees play a greater role
 - Internal Audit is showing up at a lot more meetings

Impact for FSGL (?)

- Partner relationships are held to greater scrutiny
 - Your control environment is your clients control environment
 - Increasingly likely that you meet your client's Auditors
 - Request for Audit Reports (SAS-70 equivalent)

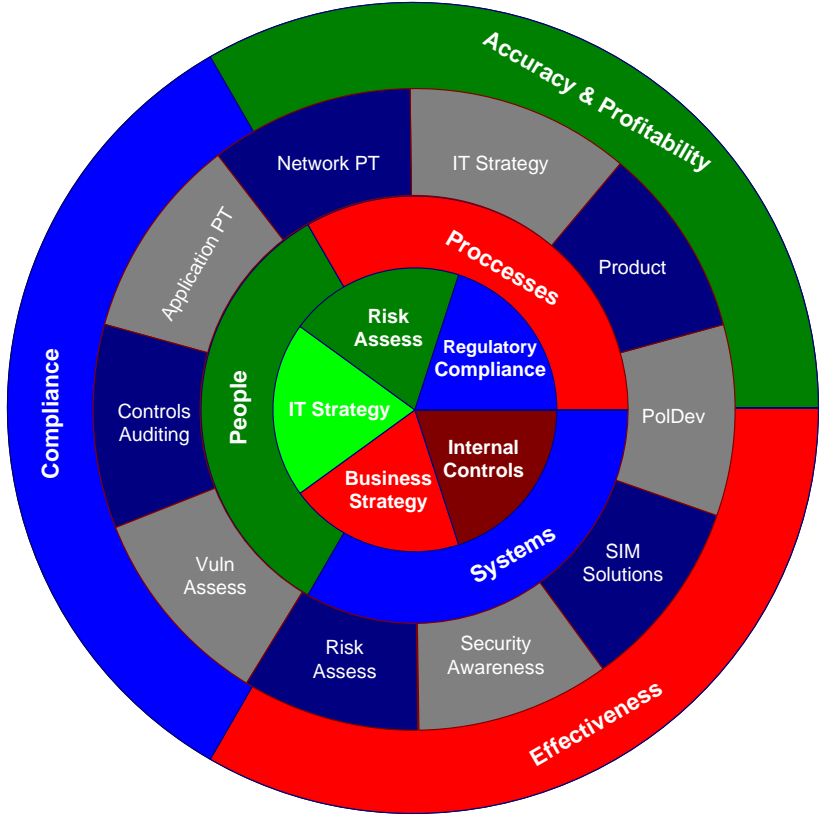
- Your relationship becomes more formal
 - Sign-off on Policies, Procedures, Standards
 - Sign-in/Sign-Out
 - Remote Access meets standards
 - Personnel held to same standards as employees

- Your Personnel need more training
 - General Security Awareness
 - Specific Regulatory Training based on client and or Systems served
 - Health Care (F5000)-- HIPAA
 - Public – Sarbanes
 - Pharma – CFR 21.11
 - Many – SB – 1386
 - Gov – FISMA
 - NJ – OPRA/GSN
 - Telco – CALEA

Open Q&A

- Presentation was intended to stimulate exchange
- Resources
 - www.itgi.org
 - www.isaca.org
 - www.sans.org
 - www.audit.net
 - www.aicpa.org
 - jverry@pvtpt.com

ABIS – IT Objectives



Objectives Specific to IT

- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability