Cyber Security Auditing for Credit Unions

ACUIA Fall Meeting

October 7-9, 2015

PIVOTGROUP
Armed with Information Security Knowledge

Topics

- **Introduction**
- **Cyber Security Auditing Program**

Discuss an effective and compliant Cyber Security Auditing Program from an:

- Internal audit department's role
- Independent External Security Auditor's Role

- **The role and effects of the IT Risk Assessments in a Cyber Security Audit Program**

Introduction

- **Jim Soenksen-CEO**
- **PIVOT Group LLC**
  - A National Independent Audit, Assessment and Compliance Firm providing exclusively Data Privacy and Protection Services
- **Offices**
  - Atlanta
  - Orlando
  - Dallas
  - Chicago- Coming Soon!

Cyber Security Audit Program DNA

DATA PRIVACY & PROTECTION

PIVOTGROUP
Armed with Information Security Knowledge

Your Obligations

- Protect Member’s Data
- Compliance
- Awareness
- Communication
- Well Informed Policy Assumptions
- Reliable Reporting
- Attestation of Results
- Current and Relevant
- Risk Based Program and Assessment

Internal Auditor’s Role

- Develop Enterprise Audit Program
  - Compliance
  - Policies
  - Internal Controls
- Independence
- Risk Base
- Leverage Departments Reporting
- Outsource as Required or Needed

Independent External Auditor's Role

- Information Security Program-Independent Attestation
- Testing areas of program where resources or expertise does not exist
- Compliance-ISO, PCI
- Special Situations
  - Validate BC/DR
  - Insider Fraud
  - Incident Response
  - Vendor Management

2015 Data Privacy Regulations

- GLBA/NCUA Reg 748 A&B
- FFIEC Authentication
- FFIEC Social Media
- PCI
- TR-39/TG-3
- State and Federal Data Breach Notification Laws
- CISPA 2015
- Enterprise Risk Management

2015 NCUA Examination Focus

- New Cyber Security Risk Exam
- IT Exam
- DDoS
- Incident Response
- BC/DR
- Enterprise Risk Management
- Vendor Management
- Remediation Progress

Check Lists

- Examination Preparation
- FFIEC Authentication Self Assessment
- New Cybersecurity Exam Questionnaire
- New Cyber Security Risk Assessment
- PCI SAQ

Biggest Voids-Internal Audit

- Expertise/Knowledge
- Interdepartmental Coordination
- Auditing Tools
- Changing Regulations/Exam Requirements
- Incident Response
- Back Up and Disaster Recovery
- IT Expertise
- Physical Security
- Board Awareness
- Risk Based
- Risk Analysis Tools

External vs. Internal

- Develop Enterprise Audit Plan
- Determine In-House Expertise and Resources
- Outsource or Train where Lack of Expertise
- Determine Required Outsource
  - Financials
  - Information Security Program
  - Website/Marketing Compliance
  - PCI

How does IT Risk Assessments Fit?

Risk Based Program

- Data Breach/Leakage
- Asset Protection
- Non-Compliance
- Reputation
- System Compromise
- Increase Costs
- Misused Resources
- Uniformed Decisions
- Missed Opportunities

Major Data Breach Prevention

- IT Controls
- Encryption
- Vulnerability Management
- Social Engineering
- Vendor Management
- Training
- Internal Fraud
- Mobile Applications Control
- Incident Response Program
- Info/Sec Control Testing
- Independent Security and Compliance Audits

Credit Union’s Biggest Threats

- Social Engineering
- Vendor Management
- Mobile Disasters
- Physical Disasters
- Insider Fraud
- Credit/Debit Cards
- Unencrypted Data
- Incident Response

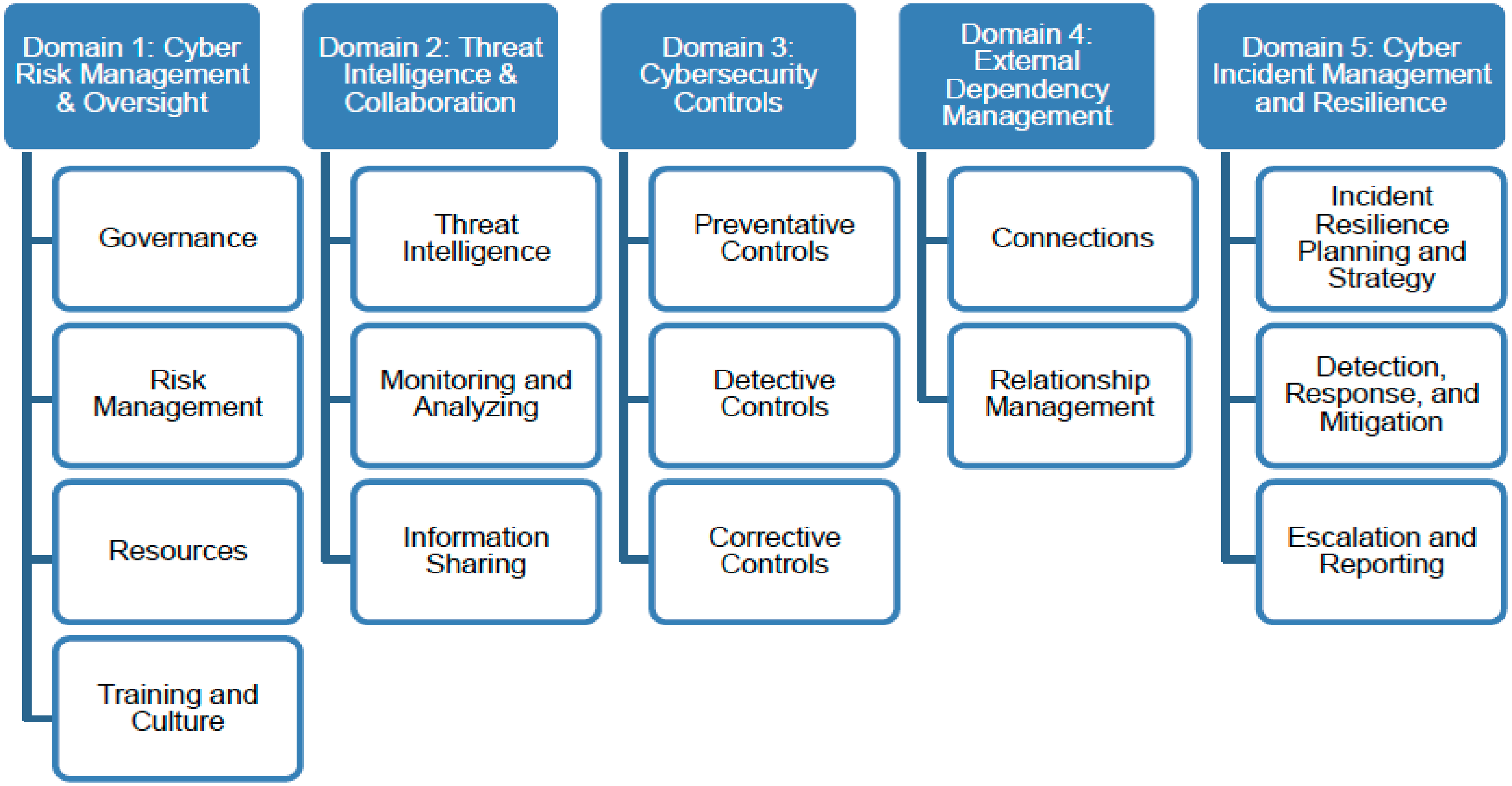
FFIEC Cyber Risk Assessment Tool

Benefits to the Institution

- For institutions using the Assessment, management will be able to enhance their oversight and management of the institution’s cybersecurity by doing the following:
- Identifying factors contributing to and determining the institution’s overall cyber risk.
- Assessing the institution’s cybersecurity preparedness.
- Evaluating whether the institution’s cybersecurity preparedness is aligned with its risks.
- Determining risk management practices and controls that are needed or need enhancement and actions to be taken to achieve the desired state.
- Informing risk management strategies

Cyber Risk Domains

DATA PRIVACY & PROTECTION



Domain 1: Cyber Risk Management & Oversight

- Governance
- Risk Management
- Resources
- Training and Culture

Domain 2: Threat Intelligence & Collaboration

- Threat Intelligence
- Monitoring and Analyzing
- Information Sharing

Domain 3: Cybersecurity Controls

- Preventative Controls
- Detective Controls
- Corrective Controls

Domain 4: External Dependency Management

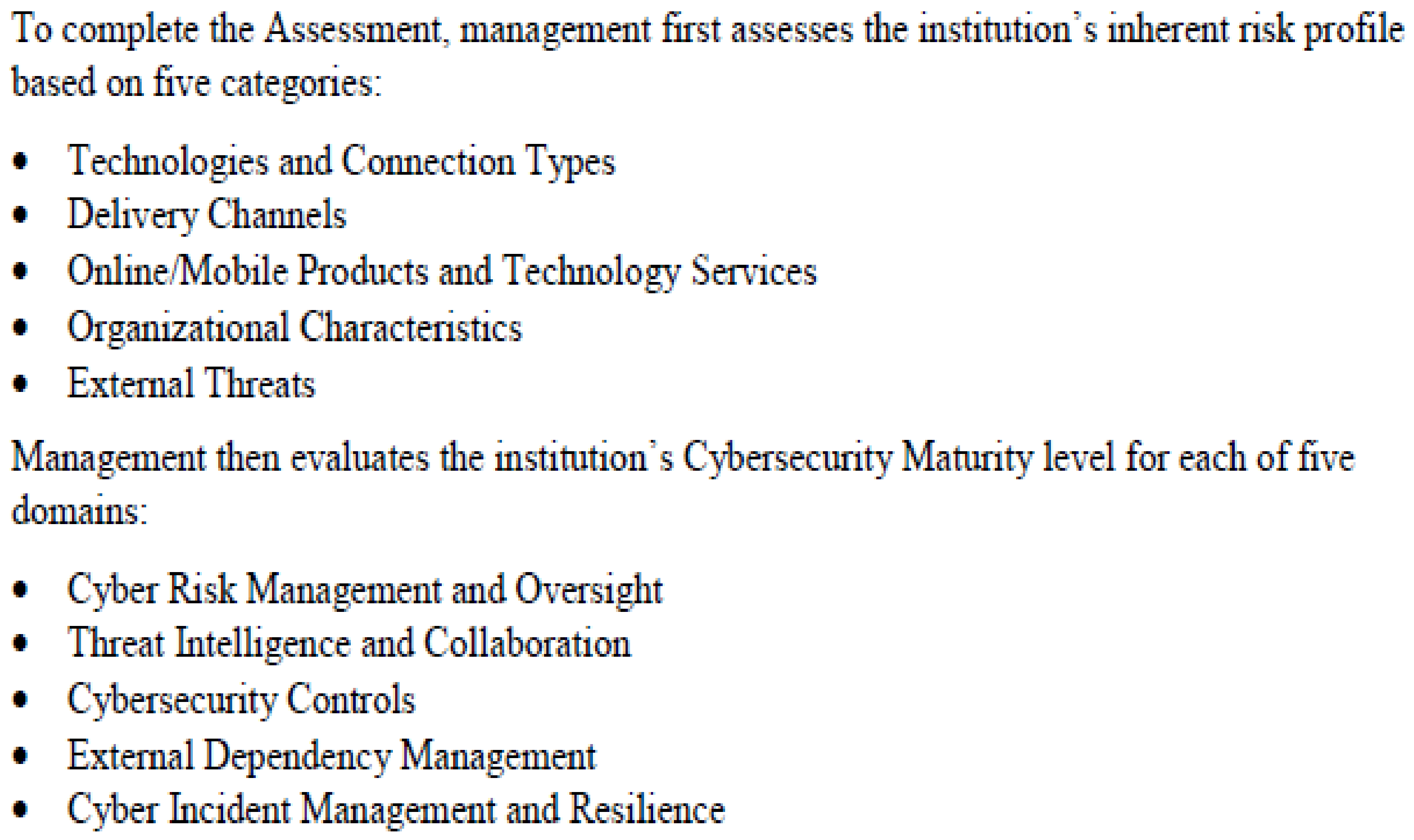
- Connections
- Relationship Management

Domain 5: Cyber Incident Management and Resilience

- Incident Resilience Planning and Strategy
- Detection, Response, and Mitigation
- Escalation and Reporting

PIVOTGROUP
Armed with Information Security Knowledge

FFIEC Cyber Risk Assessment Tool



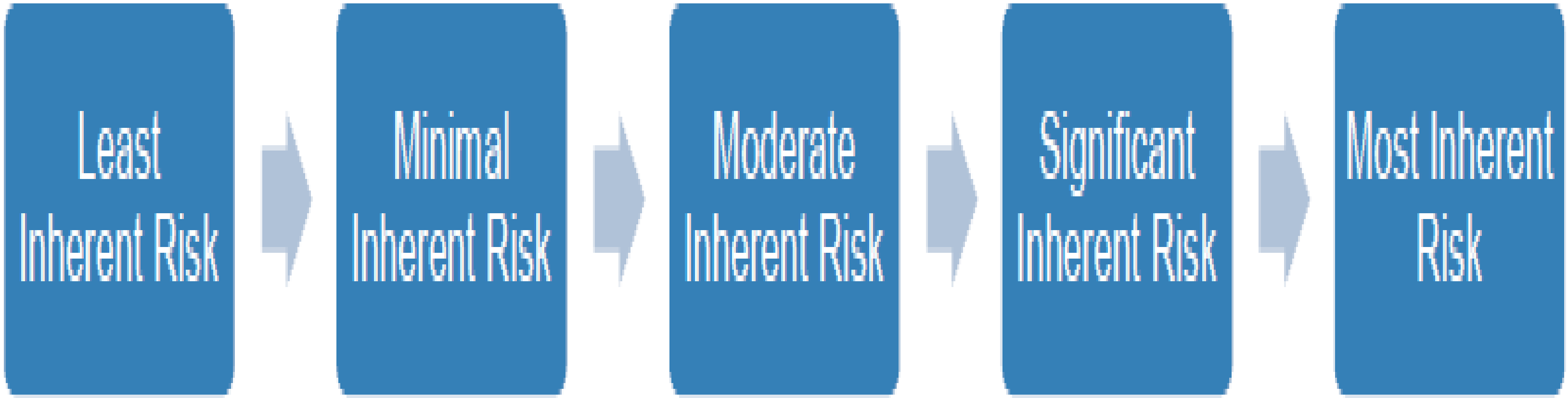
To complete the Assessment, management first assesses the institution's inherent risk profile based on five categories:

- Technologies and Connection Types
- Delivery Channels
- Online/Mobile Products and Technology Services
- Organizational Characteristics
- External Threats

Management then evaluates the institution's Cybersecurity Maturity level for each of five domains:

- Cyber Risk Management and Oversight
- Threat Intelligence and Collaboration
- Cybersecurity Controls
- External Dependency Management
- Cyber Incident Management and Resilience

Inherent Risk Ratings



Least Inherent Risk

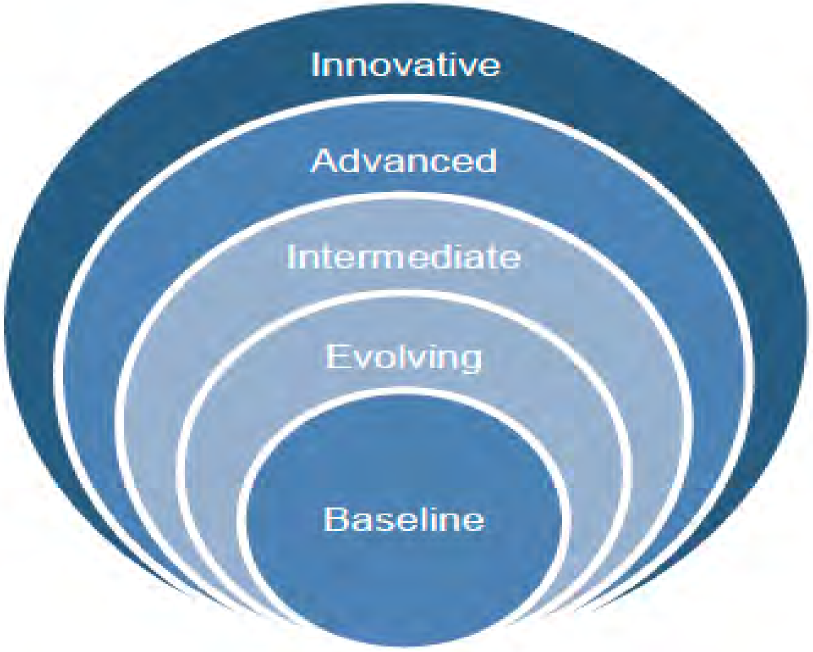
Minimal Inherent Risk

Moderate Inherent Risk

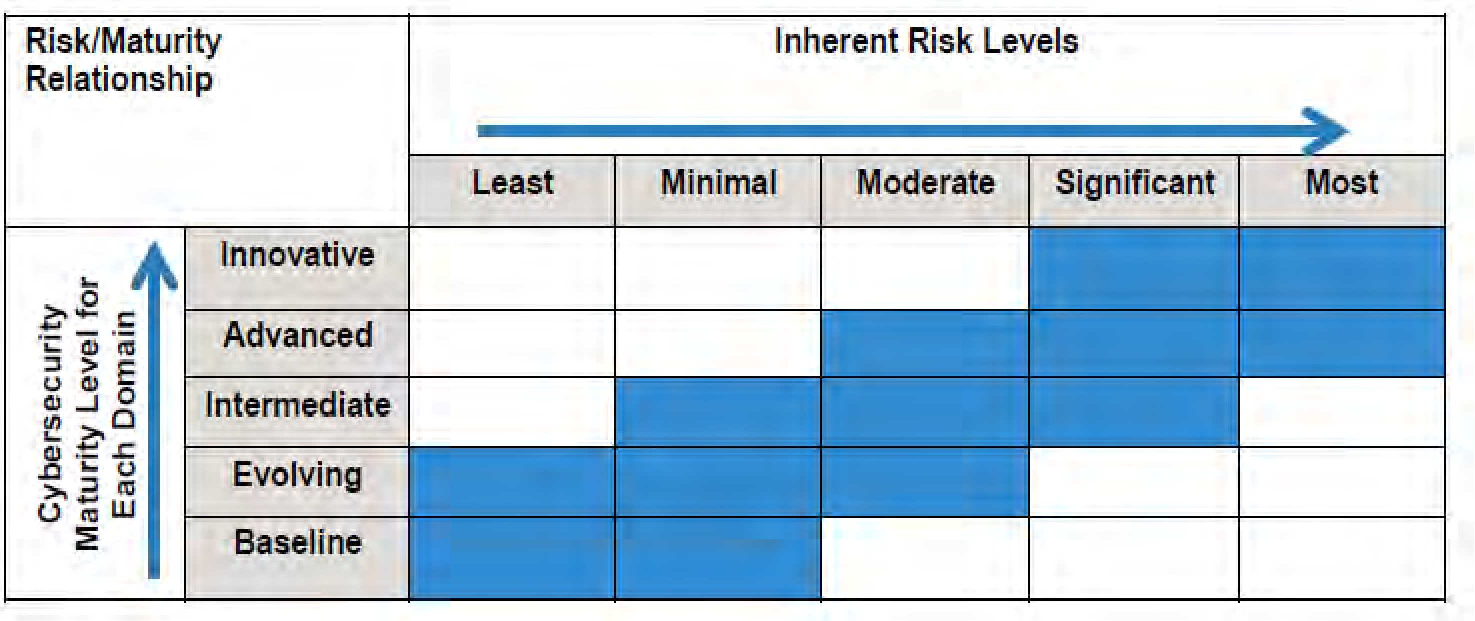
Significant Inherent Risk

Most Inherent Risk

Maturity Model

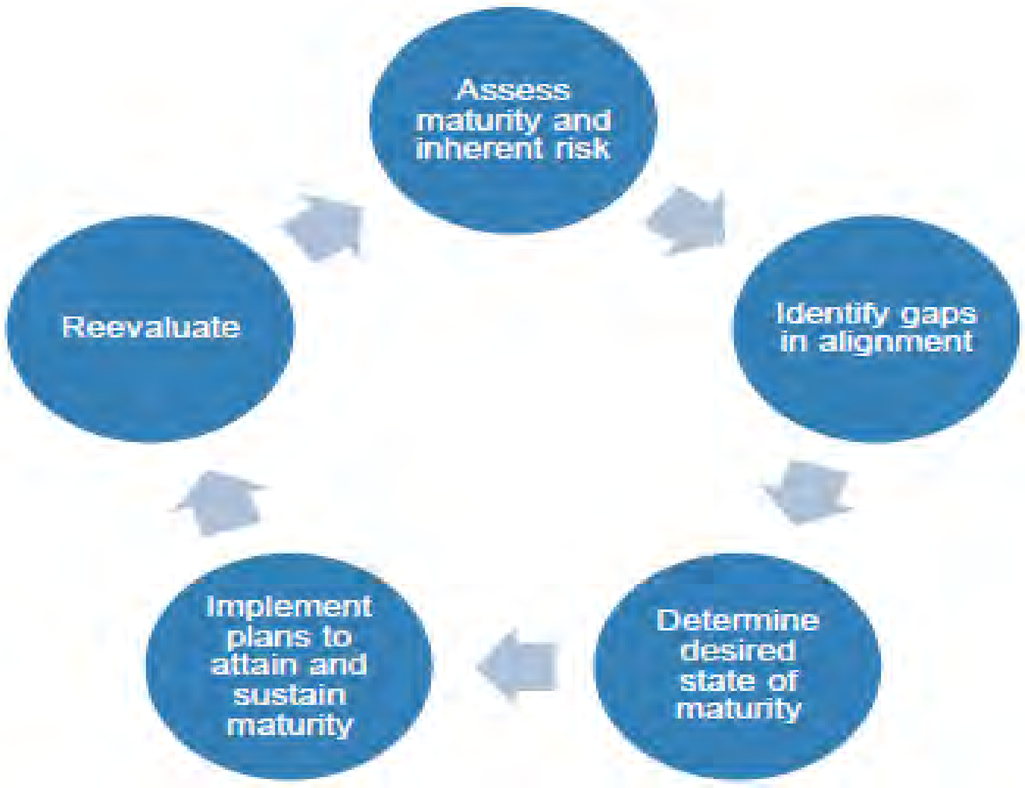


Risk/Maturity Relationship Matrix



Risk/Maturity Relationship		Inherent Risk Levels				
		Least	Minimal	Moderate	Significant	Most
Cybersecurity Maturity Level for Each Domain	Innovative				🟦	🟦
	Advanced			🟦	🟦	🟦
	Intermediate		🟦	🟦	🟦	
	Evolving	🟦	🟦	🟦		
	Baseline	🟦	🟦			

Implementation



Assess maturity and inherent risk

Identify gaps in alignment

Determine desired state of maturity

Implement plans to attain and sustain maturity

Reevaluate

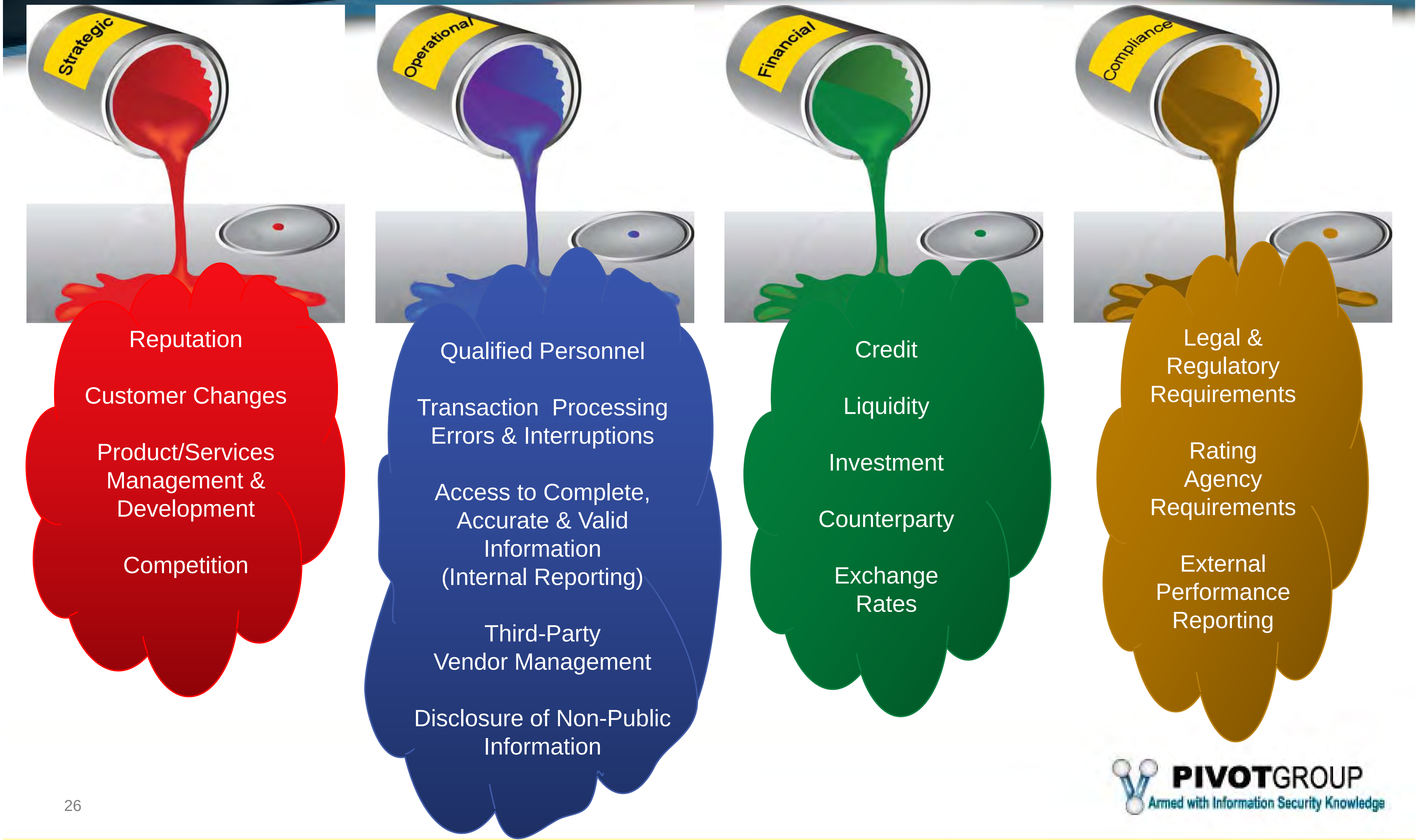
DATA PRIVACY & PROTECTION

Who does What???

PIVOTGROUP
Armed with Information Security Knowledge

Linkage to ERM

Your Risk Appetite & Profile



Reputation

Customer Changes

Product/Services Management & Development

Competition

Qualified Personnel

Transaction Processing Errors & Interruptions

Access to Complete, Accurate & Valid Information (Internal Reporting)

Third-Party Vendor Management

Disclosure of Non-Public Information

Credit

Liquidity

Investment

Counterparty

Exchange Rates

Legal & Regulatory Requirements

Rating Agency Requirements

External Performance Reporting

Take Aways

- Including Cyber Security in Internal Audit Programs
- When to Outsource
- Information Security Basics
- Cybersecurity Risk Assessments
- Integrating into ERM

Thank you!

Q&A

- Contact PIVOT Group….
  - Jim Soenksen, CEO
  - Call: 404-419-2163
  - Email: **jsoenksen@pivotgroup.com**
  - www.pivotgroup.com