

Vendor Assessments

ISACA – Geek Week

Information Technology Risk Services Group

Agenda

- **Who is in the room**
- **Varies by Industry**
- **Risks from Vendors / Suppliers**
- **Overall Approach to Vendor Assessments**
- **Risk Assessment**
- **SSAE 16 Update**
- **BITS Shared Assessments (SIG and AUP)**



Vendor Assessment Varies by Industry

- Industry Practices
 - Banks
 - Insurance
 - Healthcare
 - Manufacturing
 - Real-estate
 - Services
 - Others

positively unique



DIXON HUGHES PLLC

What are some of the risks we need to consider?

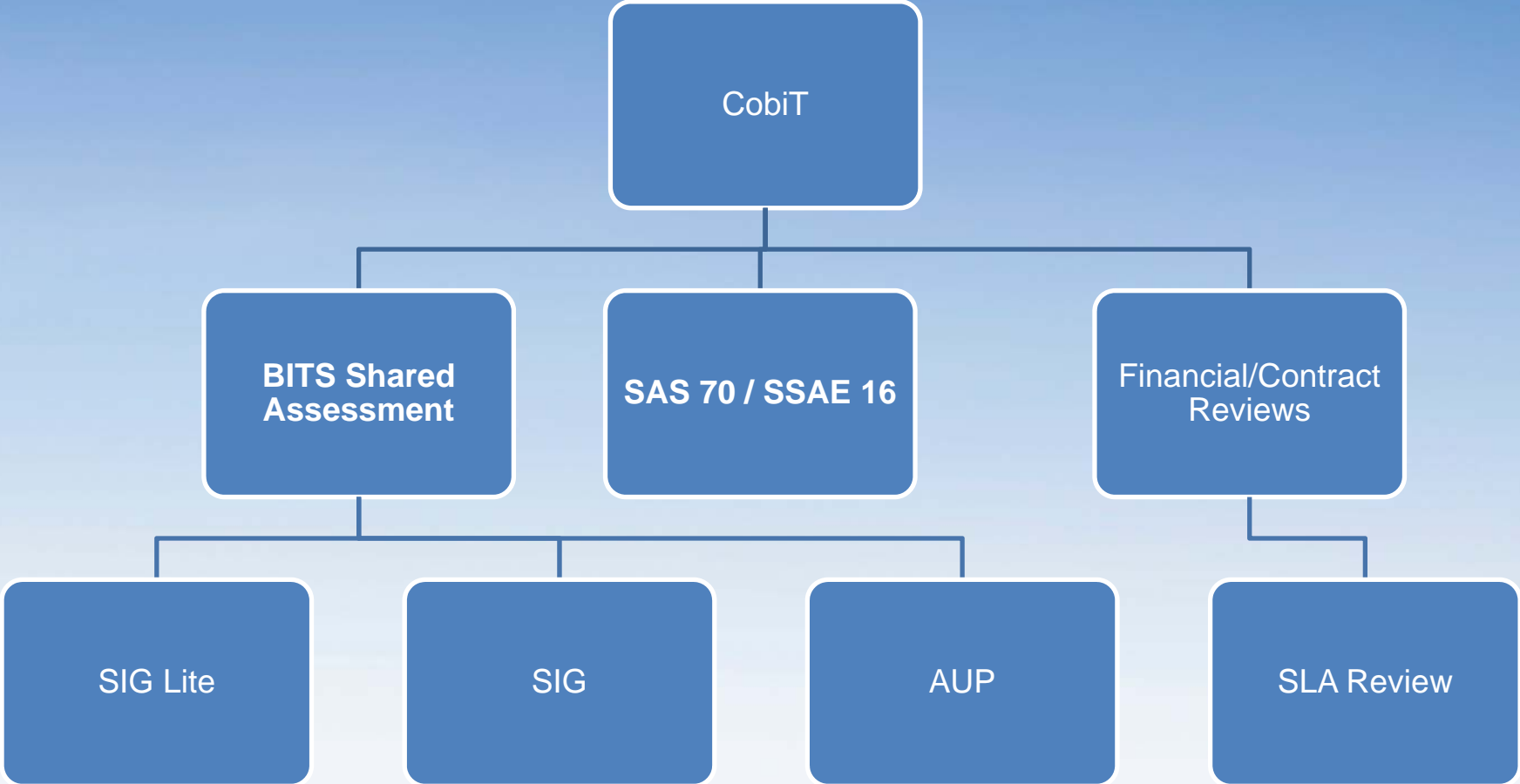
- Access to data
- Fraud / Theft
- Service Level Agreements (SLA's)
- Regulations
 - HIPPA
 - GLB
 - Sarbanes Oxley
 - FFIEC
 - FDIC
 - Privacy
 - Financial Liability
- Others?

positively unique



DIXON HUGHES PLLC

Approach



CobiT - Deliver and Support

- DS2 Manage Third-party Services
 - The need to assure that services provided by third parties (suppliers, vendors and partners) meet business requirements, requires an effective third-party management process.

positively unique



DIXON HUGHES PLLC

CobiT – DS2 Manage Third-party Services

- DS2.1 Identification of All Supplier Relationships
 - Identify all supplier services, and categorize according to supplier type, significance and criticality.
- DS2.2 Supplier Relationship Management
 - Formalize the supplier relationship management process (e.g. through SLA's).
- DS2.3 Supplier Risk Management
 - Identify and mitigate risks relating to suppliers ability to continue effective service delivery in a secure and efficient manner on a continual basis.
- DS2.4 Supplier Performance Monitoring
 - Establish a process to monitor service delivery to ensure that the supplier is meeting current business requirements and adhere to contract agreement and SLA's.

positively unique



DIXON HUGHES PLLC

DS2.1 Identification of All Supplier Relationships

Vendor	Type
BOA	Banking / Wires
Recall	Data Storage
Data Center	Systems Hosting
Card Processing	Payment Transactions
HVAC Unit Maintenance	Maintenance
Lockbox Processor	Check Processing / Deposits

- Conduct Risk Assessment on Completed Listing

Risk Assessment Criteria

- **Critical to business (1-3)**
 - 1 - Vendor would be easy to replace with a competitor
 - 2 – Cannot replace vendor without significant downtime or resource commitment
 - 3 – Our business relies on vendor to continue day-to-day operations
- **Access to Data**
 - 1 – No access to data
 - 2 – Access to data while on site (read or write)
 - 3 – Access to data from their location and / while offsite (read or write)
- **Processes Transactions**
 - Yes or No
- **Does Management Monitor SLA's**
 - Yes or No

positively unique



DIXON HUGHES PLLC

DS2.3 Supplier Risk Management

Vendor	Type	Critical to Business	Access to Data	Process Transactions	Mgmt Monitor SLA's
BOA	Banking / Wires	3	3	Yes	No
Recall	Data Storage	2	1	No	Yes
Data Center	Systems Hosting	3	2	No	Yes
Card Processing	Payment Transactions	2	3	Yes	Yes
HVAC Unit Maintenance	Maintenance	1	1	No	Yes
Lockbox Processor	Check Processing / Deposits	3	2	Yes	No

positively unique



DIXON HUGHES PLLC

Link to Vendor Assessment Spreadsheet

- Remaining CobiT Objectives addressed in the specific vendor reviews performed based on the Risk Assessment
 - DS2.2 Supplier Relationship Management
 - DS2.4 Supplier Performance Monitoring



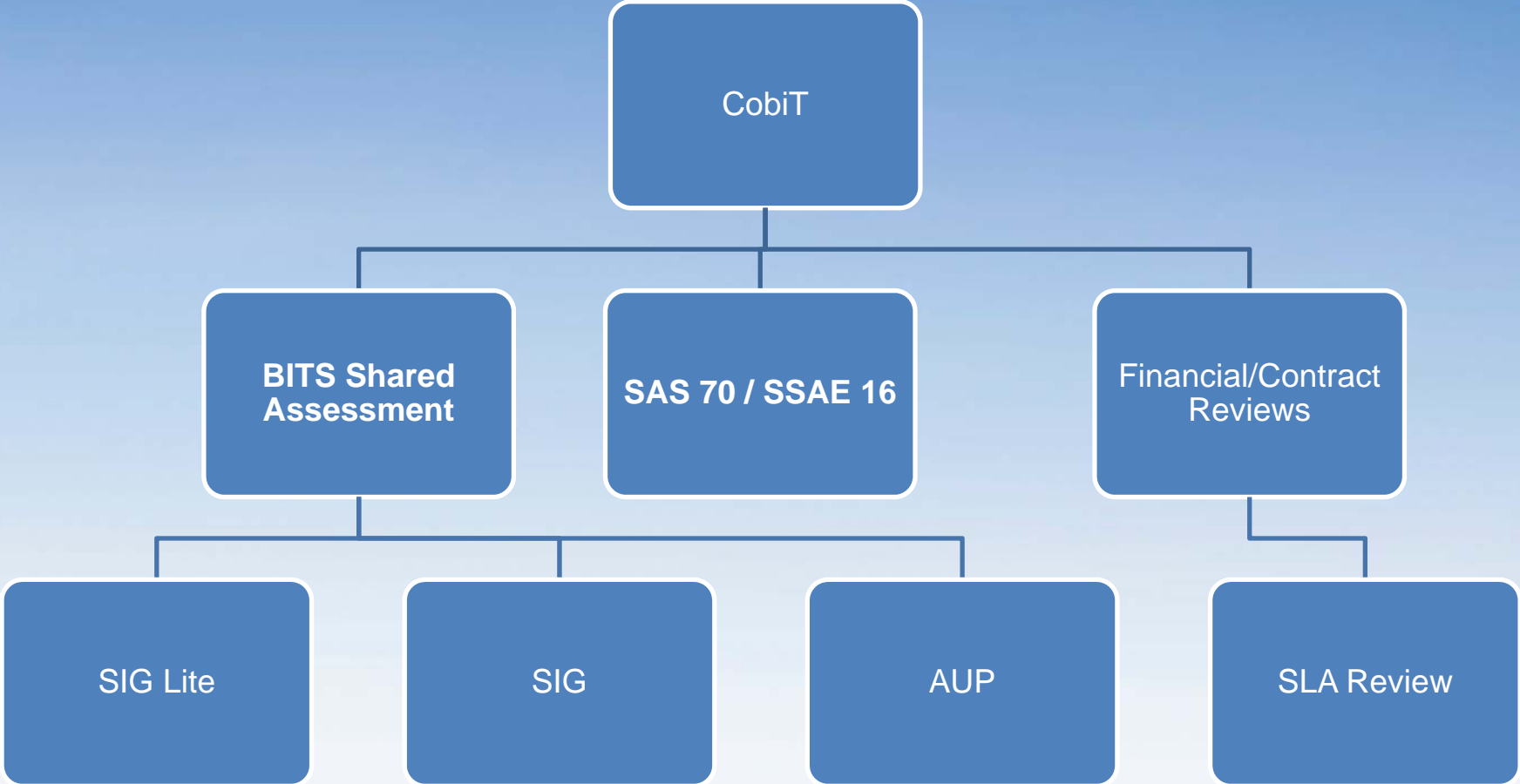
Vendor Risk
Assessment

positively unique



DIXON HUGHES PLLC

Approach



Highlights from

SSAE 16 / ISAE 3402

New Attest Standard SSAE 16 to Replace SAS 70

- Statement on Auditing Standard 70 (SAS 70) has been the US standard for auditing service organizations since it was issued in 1992. Since many US companies have service organizations outside of the country, the US standard became the de facto standard abroad, forcing some international service organizations to adhere to the US standard.
- As a result, the AICPA and the International Auditing and Assurance Standard Board (IAASB) updated their standards to provide for a consistent approach whether the service organization audit was conducted in the US or abroad.

positively unique



DIXON HUGHES PLLC

New Attest Standard SSAE 16 to Replace SAS 70

- The ensuing standards are the Statement on Standards for Attest Engagement 16, *Reporting on Controls at a Service Organization* (SSAE 16) in the US and the International Standard on Attest Engagements 3402, *Assurance Reports on Controls at a Service Organization* (ISAE 3402) outside of the US.
- Some differences between SSAE 16 and ISAE 3402...but that's for another presentation.
- The effective date of the new standard is for periods ending on or after June 15, 2011.

Some Highlights from the new Standard

- Written assertion by management of the suitability of the description, design and operating effectiveness of the Service Organization's System.
 - Management must have a reasonable basis for their assertion based on the risks that threaten the objectives.
- One opinion for description, design and operating effectiveness. Changes the coverage on the design from an as-of date to the coverage period in the Service Organization Report.
- The new standard is an attest engagement standard versus an audit standard.
- More emphasis on describing whether the inclusive or carve-out methods for controls at subservice organizations were used.

Some Highlights from the new Standard

- Minimum criteria for evaluating the description, suitability of design and operating effectiveness of the controls.
- A SAS 70 report will be referred to as a Service Organization Report.
- The Description of Services will be referred to as a Service Organization's System, and will include services provided, coverage period and control objectives.

positively unique



DIXON HUGHES PLLC

WHAT IS BITS?

What is BITS and the Shared Assessment

- BITS
 - A division of [The Financial Services Roundtable](#), BITS is a not-for-profit industry consortium whose members are 100 of the largest financial institutions in the United States.
 - Member driven, industry-standard body that injects speed, efficiency and cost savings into the service provider control assessment process.
- Shared Assessment
 - Pilot completed in 2005 / Tools launched in 2006
 - Focused on Security, Privacy and Business Continuity
 - Designed for multinationals
 - Grown beyond financial institutions
 - Tiered approach

positively unique



DIXON HUGHES PLLC

Tiered Approach to BITS Shared Assessments

- No Access to Data
 - Significant Information Gathering Lite
 - SIG Lite (i.e. data center management, janitorial services, etc.)
- Access to Data while on Site (read or write)
 - Significant Information Gathering
 - SIG (i.e. contractors/temporary employees)
- Access to data from their location and / while offsite (read or write)
 - Significant Information Gathering
 - SIG
 - Agreed Upon Procedures
 - AUP

positively unique



DIXON HUGHES PLLC

Global Privacy Initiatives

Challenges

- US: State law driving national standards, federal laws remain piecemeal (e.g. Massachusetts Information Security Regulation)
- EU: Data Protection Directive sets minimum standard, but implemented differently by member states
- Examples of other countries with data protection regulations: Canada, Argentina, Hong Kong, Australia, New Zealand
- Countries starting to adopt information security / privacy laws include India
- Asia Pacific Economic Cooperating (APEC)

Solution



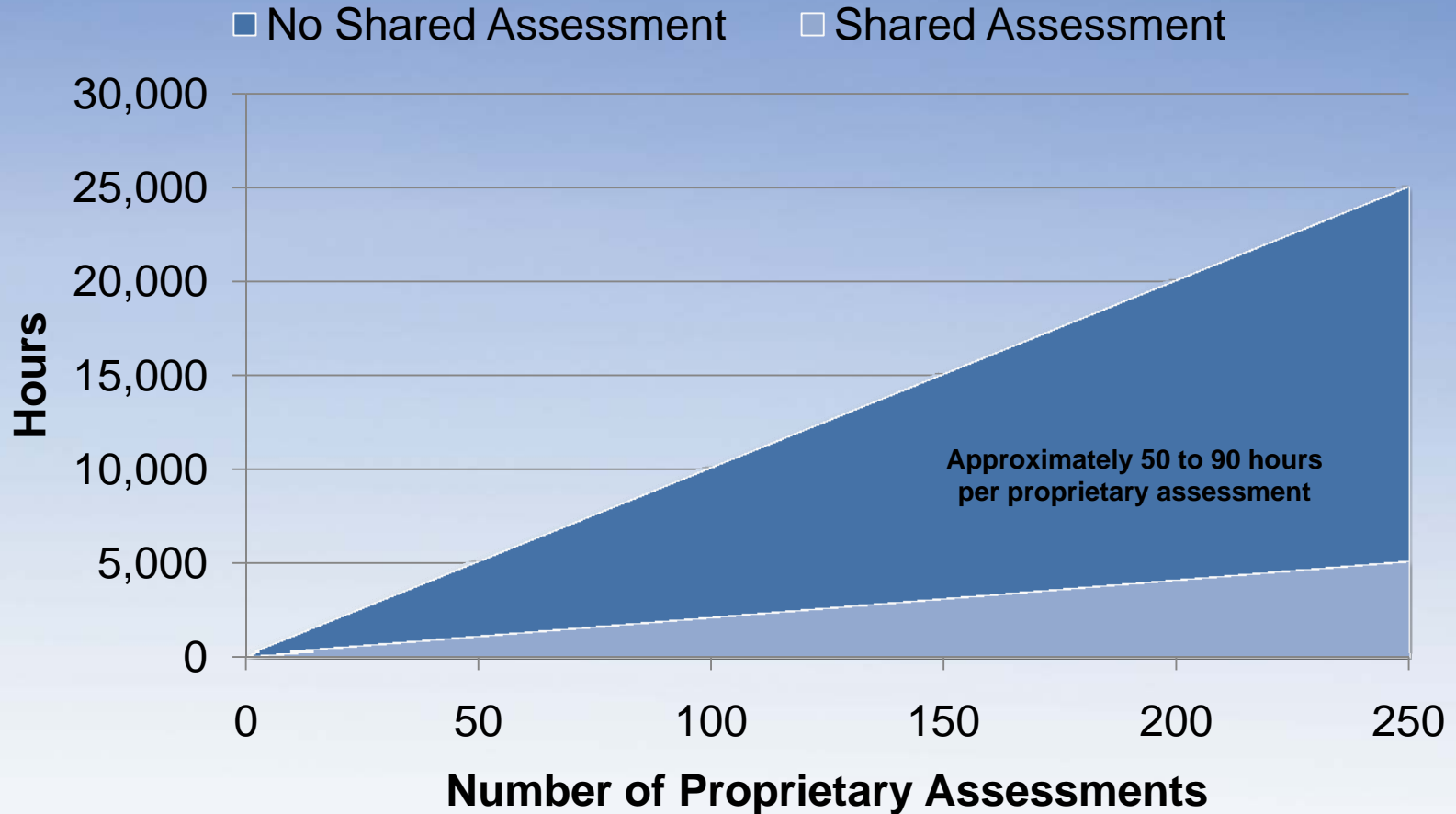
AUP Addresses - Common Themes

- Concept of personal information, protected personal information and sensitive information
- Protection for lifecycle of the data
- Privacy policies and procedures (notice, consent)
- Data handling
- Data transfers
- Information security
- Third parties (due diligence; contracts; monitoring)

SIG / AUP Version Updates

- SIG and AUP versions are released annually to address emerging risks and trends.
- Version 4 Released in 2008 Aligned Shared Assessments Program to industry standards
 - ISO 27002:2005
 - COBIT
 - PCI DSS
 - FFIEC
- Version 5 released in 2009 expanded education and outreach to strategic foreign countries through organizations such as NASSCOM
 - NASSCOM® is the premier trade body and the chamber of commerce of the IT-BPO industries in India.
- Expand awareness and adoption to other sectors (e.g. Healthcare, Retail, Telecom, Higher Education)

Industry Example of Reliance on SIG / AUP



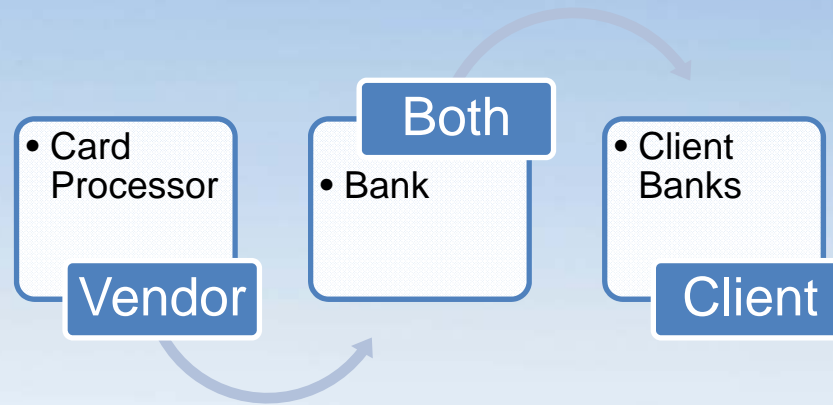
positively unique



DIXON HUGHES PLLC

Shared Assessment Success Factors

- Education
 - To begin the process you must be sure to educate all involved in the process of what is going to happen and why
 - Be sure to consider upstream and downstream



- Find an Executive Level Champion

Shared Assessment Success Factors

- Standardized Information Gathering (SIG)
 - Define scope
 - Regions, countries, product lines
 - You don't want to get started and get confused
 - Complete inventories of hardware and software
 - Inventories for hardware and software are used throughout the AUP for sampling
 - Not having complete inventories for in-scope areas can bring your progress to a halt!

positively unique



DIXON HUGHES PLLC

Shared Assessment Success Factors

- AUP Process
 - Plan, plan and plan.....multiple stakeholders throughout the organization
 - Prepare Document Request List Ahead of Time
 - Execute Testing
 - Draft Report
 - Management Review and Response
 - Issue Report
- Now, lets walk through the Shared Assessment

positively unique



DIXON HUGHES PLLC

SIG and AUP Section Overview

- A. Risk Management
- B. Information Security Policy
- C. Organization of Information Security
- D. Asset Management
- E. Human Resources Security
- F. Physical and Environmental Security
- G. Communications and Operations Management
- H. Access Control
- I. Information Systems Acquisition, Development and Maintenance
- J. Information Security Incident Management
- K. Business Continuity Management
- L. Compliance
- P. Management of Privacy Program

positively unique



DIXON HUGHES PLLC

SIG and SIG Lite Revisited – Executing

- Mock Questionnaire



SIG - Full - V.5

AUP Revisited – Executing

- AUP Format
- Sampling Methodology
- Practitioners Notes
- Glossary



AUP V.5

Contact Information

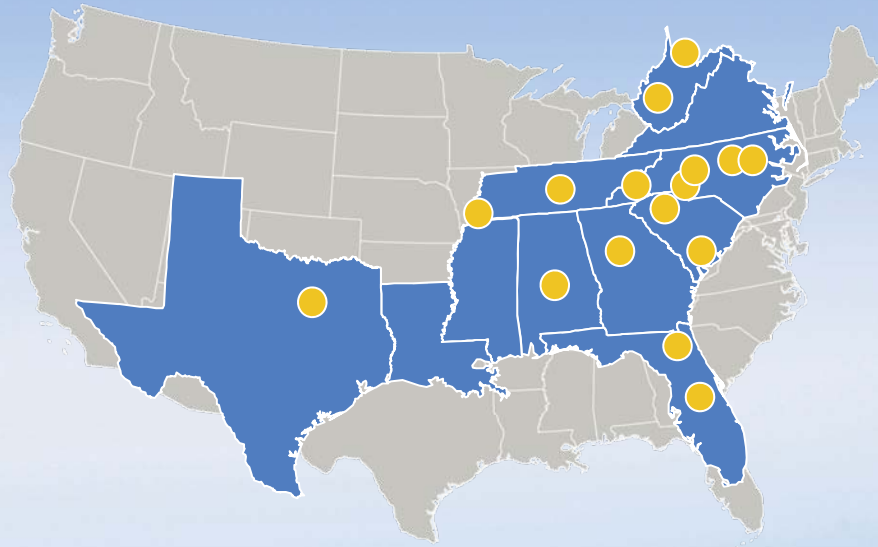
PATRICK CATTON, CIA, CISA, CGEIT

- pcatton@dixon-hughes.com
- 404-575-8997
- 404-354-5298

ANDREW MCIVER, CIA

- amciver@dixon-hughes.com
- 404-575-8842
- 205-310-7589

Dixon Hughes PLLC Reach



- 1,000+ People
- 22 Cities / 8 States
- Largest headquartered in Southeast
- U.S. top 15 auditor of larger public companies

Dixon Hughes dominates the Southeast and does business in all 50 states.

Dixon Hughes offices



Alabama Florida Georgia North Carolina South Carolina Tennessee Texas West Virginia

positively unique



DIXON HUGHES PLLC

International Alliance



Member of Praxity, an international alliance of independent accounting firms that offers multinational clients access to resources around the world.

- Global Ranking: 8th
- 4 largest U.S. member firms (including Dixon Hughes) if combined would rank as 6th largest U.S. accounting firm
- Revenue: \$3.2 billion
- 101 firms with more than 24,000 staff in 72 countries

