Maintaining Compliance Over Service Providers

Sumit Kalra
Burr Pilger Mayer, Inc.

September 5, 2012

BPM
BURR PILGER MAYER
Accountants and Consultants

Agenda

- Definitions
- Current State
- Outsourcing
- Compliance Drivers
- Risks and Exposures
- Compliance Strategies (Customer’s To-Dos…)
- Compliance Reporting Considerations
- Service Organization’s Perspective
- Reporting and Certification Options
- Assessment Frameworks
- Service Organization Compliance as a Process

Definitions

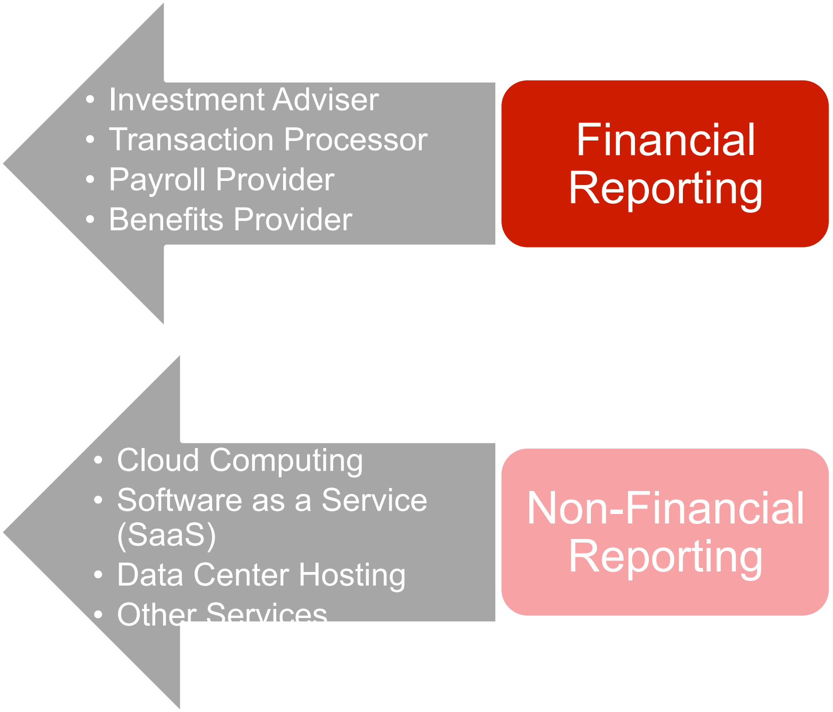
- Service Organization – Service Provider
- User Organization – Customer
- User Organization’s Auditor/Information Security Team/ Compliance Team – Customer Stakeholders
- Service Organization Auditor – Independent Third-party

Current State

Outsourcing

Service Organization

User Organization



- Investment Adviser
- Transaction Processor
- Payroll Provider
- Benefits Provider

Financial Reporting

- Cloud Computing
- Software as a Service (SaaS)
- Data Center Hosting
- Other Services

Non-Financial Reporting

1. **Efficiency**
2. **Speed**
3. **Expertise**
4. **Agility**
5. **Cost Effectiveness**

1. **Efficiency**
2. **Speed**
3. **Expertise**
4. **Agility**
5. **Cost Effectiveness**

Outsourcing

- Traditional Form
  - Mostly Common in Private Sector.
  - Enough Controls at the Customer (Supervisory Level) to minimize risk and exposures. i.e. Quality assurance, reconciliation, user acceptance.
- Primary Functions
  - Manufacturing, Packaging and Shipping
  - BackOffice Administration and Transaction Processing
  - On-site People and Technology Sourcing

Outsourcing

- Current Form
  - Private and Government Sectors.
  - Multi-tenant Environments with Controls almost absent at the Customer.
- Primary Functions
  - Internal Business Functions – Payroll, HR, Benefits Administration, Transaction Processing, Inventory Management, Fulfillment, CRM, Business Intelligence, Printing, Marketing, etc.
  - Business Technology – Microsoft 360, Google Aps, etc.
  - Customer Facing Environments – Infrastructure, Managed Services, Hosting, Customer Data Storage, Application Development, Communication, etc.

Compliance Drivers

- CUSTOMER
  - Mitigate inherent risks with outsourcing
  - Provide transparency
  - Facilitate risk management
- REGULATION/REGULATORS
  - Industry Specific – SOC, PCI, etc.
  - Federal Government – SOX, HIPAA, FISMA, A133, Energy Reduction Mandates
    - Gas and Electric rebate programs, other Federal/State initiatives
  - State/Local Government –Most long term programs
    - Privacy requirements, secure money transmission, child support collections/ payment processing, tax match services, court services

Risks and Exposures

- Data Integrity
- Information Management
- Security
- Systems Operations
- Disaster Recovery
- Regulatory Compliance
- Business Continuity
- Intellectual Property Rights
- Privacy
- Ownership
- Right to Audit Clause
- On-shore or Off-shore
- Confidentiality
- Licensing
- Limitations of Liability
- Sub-sourcing
- Reputation
- Fiduciary Responsibility
- Exist Strategy
- Many, Many, Many more…

Compliance Strategies (Customer's To-Dos…)

- Preventative – Initial and Ongoing
  - Perform Due-diligence and Manage Contracts
  - Understand Roles and Responsibilities
  - Define SLAs and measurement criteria
  - Know your Exit Strategy
  - Document Risks and Implement Mitigation Controls
- Detective
  - Implement Supervisory Controls
  - Monitor SLAs
  - Review on-going assessments
- Corrective
  - Push for change at the Service Provider…

Compliance Reporting Considerations

- Scope
- Testing Methodology
- Design Effectiveness
- Point in Time Verification
- Roles and Responsibilities Boundaries
- Operating Effectiveness Over a Period of Time
- Self Evaluation vs. Independent Assessment

Service Organization's Perspective

- Sales team's key objectives:
  - Dominate the market
  - Meet the Customers needs and gain trust
    - Cost, Compliance, Flexibility
  - Distinguish themselves from the competitor
- Operations and Development team's key objectives:
  - Enable Customers to manage risks and exposures
  - Cost reduction through standardization of processes
  - Ensure processing integrity and data reliability
  - Minimal deviation from standard processes to ensure cost management

Service Organization’s Perspective (cont.)

As a result, Service Organizations can choose to undergo…

- ❖ Independent audit /assessments under various standards and frameworks.
- ❖ Demonstrate consistent application of relevant internal controls.
- ❖ Minimize the customer’s need to perform initial and on-going due-diligence audits.
- ❖ Transparency with customers on compliance and audit results.

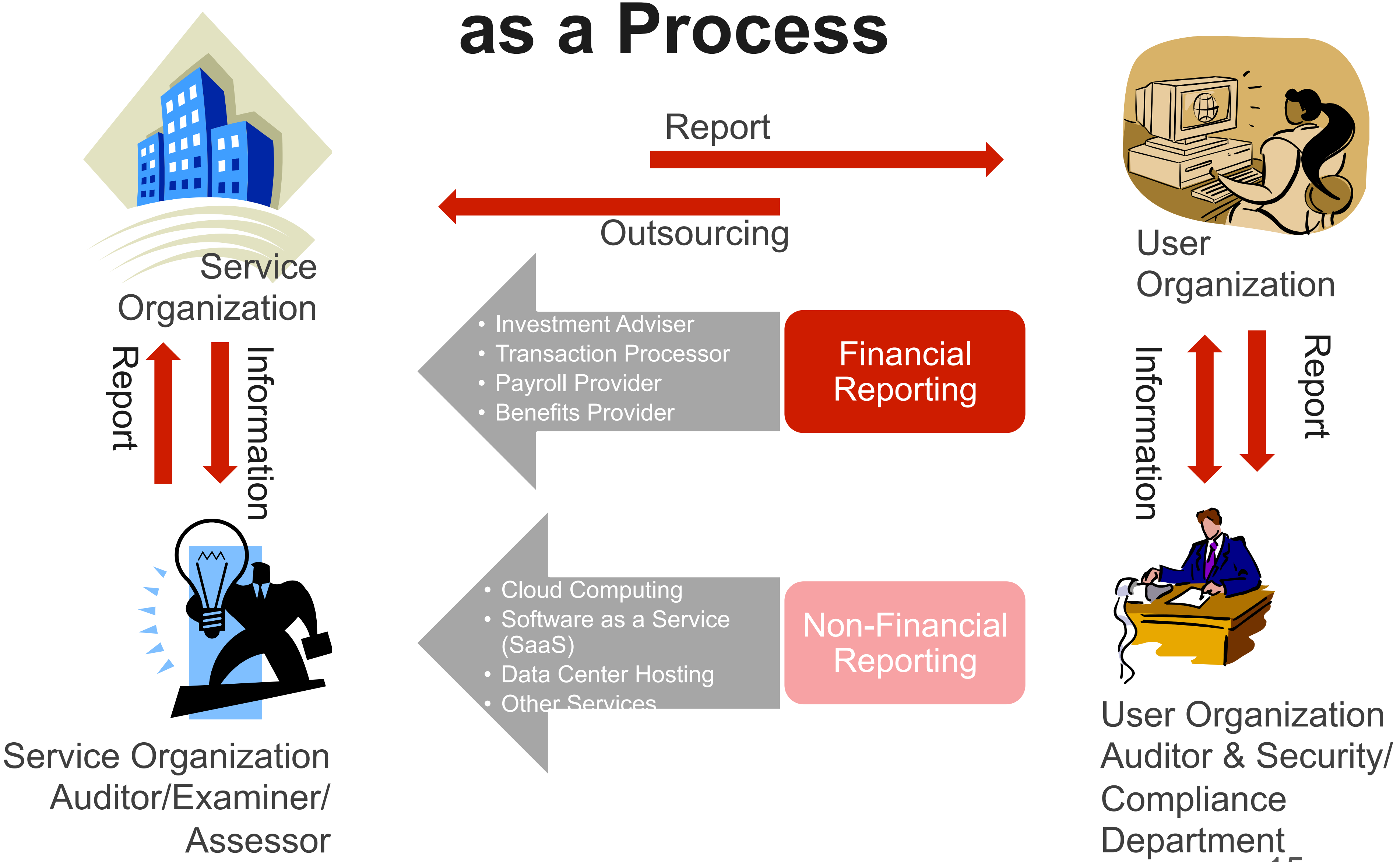
Reporting/ Certification Options

Frameworks	**Subject Mater**
SSAE 16 (SOC 1, 2, and 3)	*ICFR and Trust Services Principles Criteria and Illustrations*
ISAE 3402 and 3000	International Equivalent of SSAE 16 SOC 1 and SOC 2 respectively.
PCI	Payment Card Industry Standard
HIPAA, HiTech, HiTrust, etc.	Healthcare
ISO 27000	General Information Security
NIST 823/FISMA/Fed Ramp	United States Federal Government
CSA	Cloud Assessments

Service Organization Assessment Frameworks

- COBIT – 4 and 5
- IIA GTAG 7
- ISO 27001 and 2
- ITIL
- CMM
- COSO
- PCI
- FedRamp/FISMA NIST 823
- WebTrust

Service Organization Compliance as a Process



Service Organization

Outsourcing

Report

User Organization

- Investment Adviser
- Transaction Processor
- Payroll Provider
- Benefits Provider

Financial Reporting

- Cloud Computing
- Software as a Service (SaaS)
- Data Center Hosting
- Other Services

Non-Financial Reporting

Report

Information

Information

Report

Service Organization Auditor/Examiner/ Assessor

User Organization Auditor & Security/ Compliance Department

Sumit Kalra, Director

415.999.4553

SKalra@bpmcpa.com