“The 7 Deadly Sins of SAS 70’s”

Presented by:

Christopher Mitchell, MBA, CIA, CISA, CCSA

Seven Deadly Sins

- Lust (obsessive or excessive thoughts)
- Gluttony (over-indulgence)
- Greed (sin of excess)
- Sloth (uneasiness of the mind)
- Wrath (hatred or anger)
- Envy (insatiable desire)

Points of Discussion

- ☑ Who needs a SAS 70 assessment?
- ☑ What are the steps in the SAS process?
- ☑ Preliminary preparation for a SAS 70 assessment
- ☑ Common issues found during a Type II assessment
- ☑ Benefits of a SAS 70 Report
- ☑ Open discussion and questions

Who needs a SAS 70 Report?

Service providers who serve public and private companies by providing a service that materially impacts the company's financial statements will be required by their customers to provide a SAS 70 report.

What is a Service Organization?

Providing services that impact a customer (or “user”) organization’s internal control

- ☑ Organization that host or support customer hardware and software.
  - Data center providers
  - Application service providers (ASPs)
  - Managed information security services
  - Web-hosting or eCommerce infrastructure services
- ☑ Organizations that assist customers with initiating, authorizing, recording, or processing transactions.
  - Transfer agents and custodians
  - Third-party administrators (TPAs)
  - Claims processing facilities
  - Data warehouses
  - Call center and customer service centers

SAS 70 Examination

- The AICPA's Statement on Auditing Standards No. 70 (SAS 70) "Service Organizations" provides your customers and their auditors information to assist them in evaluating the system of internal control related to your services.
- There are two types of SAS 70 reports:
  - Type I Reports
  - Type II Reports
- Usually a minimum period of six months will be reviewed for Type II Reports.

SAS 70 Examination

Evaluating service organization controls

- Type I Reports are designed to provide information regarding:
  - Controls over relevant systems and the underlying technology at your organization.
  - Whether such controls were suitably designed and had been placed in operation as of a point in time.
  - No detailed testing of controls is performed.
- CPA firm concludes and gives an opinion on the controls placed in operation as of a point in time and the effective design of those controls.

SAS 70 Examination

Testing the operating effectiveness of controls

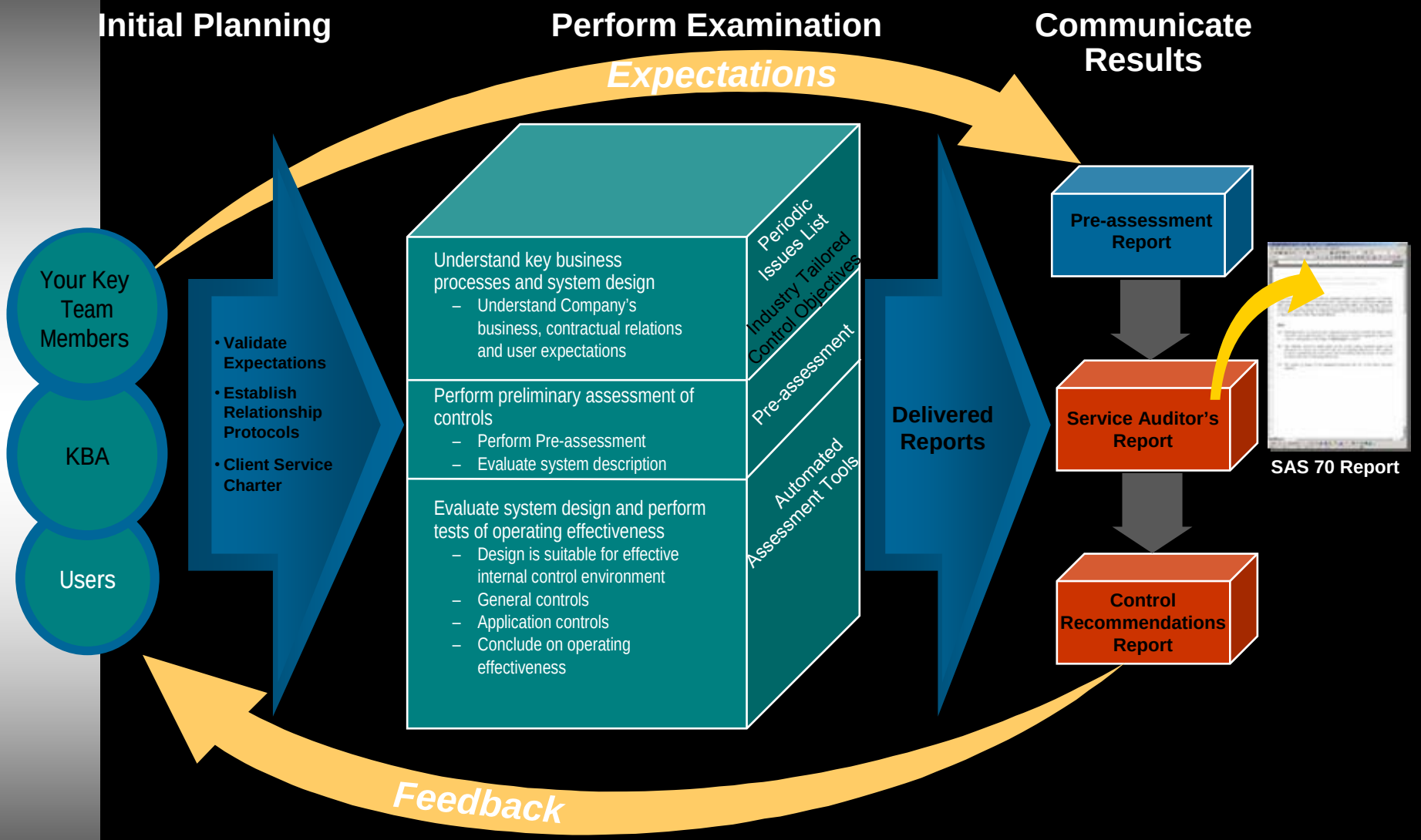
- ☑ Type II Reports provide additional information about the nature, timing, extent, and results of the service auditor's tests of specified controls at your organization. This information is highly useful to your customers and their auditors.
- ☑ The purpose of this review is to provide reasonable, but not absolute, assurance that the identified controls are operating with sufficient effectiveness during the examination period.
- ☑ User auditors can place reliance on the results from the Type II procedures.
- ☑ External Auditor concludes and gives an opinion on the controls placed in operation and the operating effectiveness of those controls during a minimum six-month period.

SAS 70 Examination

Scope and description of controls

- ☑ Services that would be considered part of the customer organization's information system would be included in the scope of the examination.
- ☑ Management is responsible for preparing a description of controls that provides user auditors with enough information to plan their own audits.
- ☑ The description of controls generally includes the following:
  - Aspects of the service organization's control environment; risk assessment; monitoring; and information and communication processes.
  - Control objectives and related control activities.
  - Complimentary controls at user organizations.
- ☑ Control objectives generally address key processes such as application development and maintenance; logical access and security; data transmission security; physical access and security; and transaction processing.

KBA SAS 70 Methodology



Common Issues Discovered

- Policies and Procedures not defined, documented and communicated
- Roles & Responsibilities not defined and documented
- Key personnel are not adequately trained on job responsibilities
- Control gaps are not timely resolved
- Lack of segregation of duties
- Lack of adequate controls around change management
- Inappropriate access to the key applications and the network

SAS 70 Benefits

What is gained from this service?

Benefits – Service Provider

- ☑ Respond to Sarbanes-Oxley inquiries
- ☑ Marketing tool to potential clients
- ☑ Stronger Control Environment
- ☑ Eliminate or mitigate repeat audits
- ☑ Independent assurance
- ☑ Client service
- ☑ Competitive expectation
- ☑ Process improvement

Benefits – Users

- ☑ Provides information to assess the overall control environment for customer (user) auditors
- ☑ Satisfy certain client Sarbanes-Oxley 404 requirements
- ☑ Recommended user controls
- ☑ Can control some audit costs
- ☑ Provides time efficiencies to customer auditors by already having information available/prepared

Questions?