



FRAZER  
FROST, LLP  
Certified Public Accountants

# Internal Controls

Cody Griffin CPA, CITP, CISA

Risk Assurance Services



# Content

- Common SAS 115 Comments
- Common Applications
- Outsourcing /Cloud Computing
- SAS 70
- Control Basics
- IT General Controls
- The Bull's Eye

# \* Common SAS 115 Comments Business Process Controls

Percentage	Finding / Risk
33%	Due to the limited number of employees working at the buying sites, many of critical duties are combined and given to the available employees. Presently, a single individual prepares and signs checks as well as maintains the general ledger.
20%	At the time of our audit, there were several large checks that had been outstanding for several months. Tracking outstanding checks is an important control procedure that ensures that all outgoing checks are accounted for.
13%	One person is responsible for preparing payroll input, reviewing the payroll journals from the payroll system, finalizing each payroll for employees and amounts, determining the bank transfer and distribution of bank transfer to the employees accounts for each payroll. This combination of duties is completely incompatible and significantly increases the chance of an error or irregularity going undetected.
13%	During the review of internal control processes related to AP we noted that all employees with access to the AP module also maintained the ability to create vendors.

# \* Common SAS 115 Comments

## General Computer Controls

Percentage	Finding / Risk
60%	Passwords to log onto the network / financial application(s) are not required to change (expire) periodically.
60%	Backup media is not being rotated off site to an environmentally and physically secure location. Backup media is not being tested periodically to ensure recoverability.
47%	The CFO/Controller have administrator rights to the financial application(s).
40%	Access to the physical location of the computer hardware is not restricted.
40%	Written disaster recovery procedures do not exist.
33%	While many IT and operational procedures are standardized and routinely followed, they have not been documented and approved by management.
27%	Segregation of duties does not exist within the financial application
20%	Shared users IDs are being used.
13%	An evaluation of the outside service provider's SAS 70 Type II report is not being conducted.
1%	User access within the financially significant applications is not being reviewed periodically.
1%	Programmers have access to the live application's source code / supporting data, and change documentation is not standardized.



# Common Applications

## ERP

Custom (Unix)

Dynamics

Farm Business Software (FBS)

Macola

MAS200

MAS90

Peachtree Quantum

Platinum

Taylor Made Solutions



# Common Applications

Live Inventory

Dynamics

Farm Business Software (FBS)

Lot Tracker

Macola

MAS200

MAS90

MTech

PigKnows

ProTrack

Taylor Made Solutions



# Common Applications

Feed Mill

Agris

CTN Data

Dynamics

Feed Office Pro

Repete

Taylor Made Solutions

WEM4000



# Common Applications

Payroll

ADP

CompuPay

Custom (Unix)

Evolution

Farm Business Software (FBS)

Macola

MAS90

Platinum

Redwing

Taylor Made Solutions

WebPay



# Outsourcing / Cloud Computing

- What controls do you have in place?
- Do you still own your data?
- What happens if you decide to change providers?
- Did you have an attorney assist with the contract?
- Do they have a SAS 70?

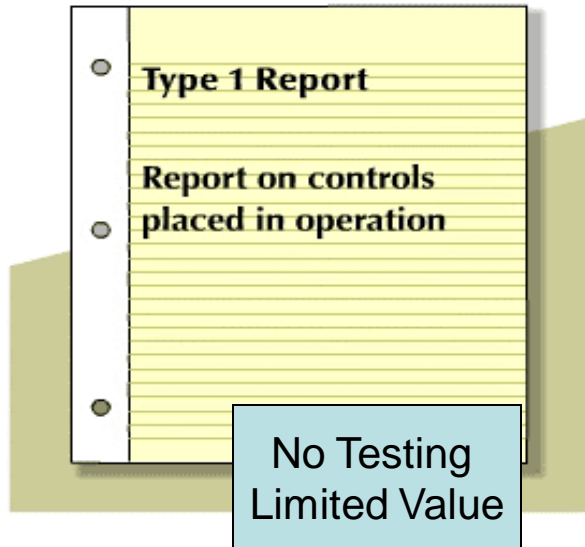


# SAS 70

- A SAS 70 audit is a process in which an independent accounting firm assesses the internal controls of a service organization and issues both a service auditor's report and an opinion based on the assessment.
- Service auditor reports are referred to as SAS 70 reports because they are defined by Statement on Auditing Standard (SAS) No. 70 issued by the American Institute of Certified Public Accountants (AICPA).



# Type 1 vs. Type 2 Report

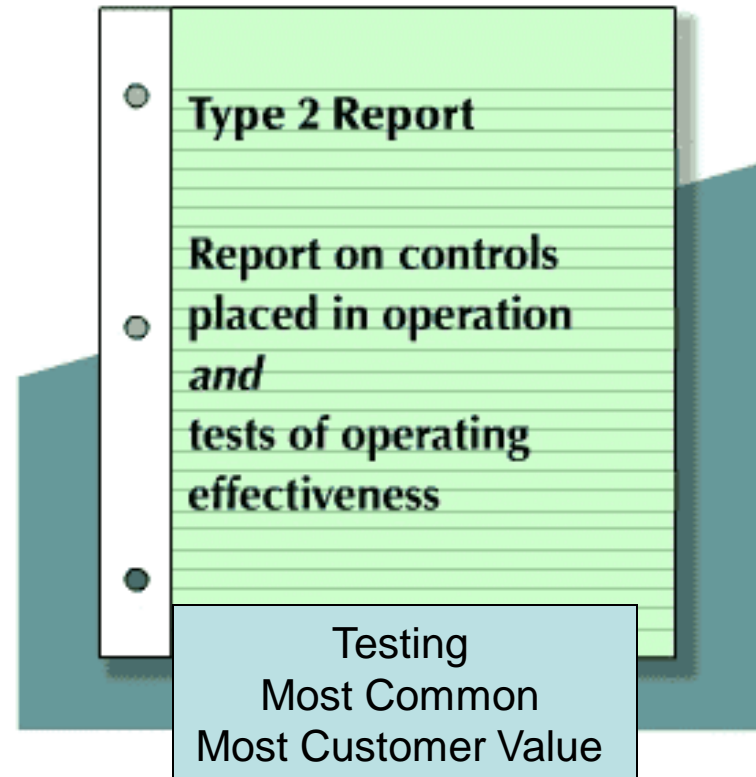


- **Type 1 Report:** A service auditor's report on the fair presentation of a service organization's *description* of its controls that *may be relevant* to a user organization's internal control as it relates to an audit of financial statements, on whether such controls were *suitably designed* to achieve specified control objectives, and on whether they had been *placed in operation* as of a specific date.



# Type 1 vs. Type 2 Report (cont.)

- **Type 2 Report:** provides a *description* of the controls that *may be relevant* to a user organization's internal control as it relates to an audit of financial statements, on whether such controls were *suitably designed* to achieve specified control objectives, on whether they had been *placed in operation* as of a specific date, *and* on whether the controls that were tested were operating with sufficient effectiveness to provide *reasonable*, but not absolute, *assurance* that the related control objectives were achieved during the period specified.





# Importance of User Control Considerations



# \* User Control Considerations: What are they?

- Controls important to the process but that are left to the responsibility of user organization
- Outside the scope of the controls the service organization can provide
- Guidance for user auditor for controls to test at the user organization



# User Control Considerations: How do they help service organizations?

- Clearly Define Responsibility: If the control cannot be maintained internally it provides a way to notify user that they are responsible for the control.
- Limit Liability: User control considerations help more clearly define where liability for controls is situated.



# Identification of controls

Question: **What is a control?**

*Answer:* A control is an activity put in place to mitigate a risk.

Question: What types of risks should we be thinking about in our work?

*Answer:* The risk that Financial Statement Assertions and Information Processing Objectives are not met.



# Think controls!

What words are often associated with controls?

- Match
- Review
- Re-perform
- Compare
- Restrict
- Validate
- Reconcile



# Control Evaluation Questions

- Automated or Manual
- Close to process or far from process
- Close to accounts or far from accounts
- Control has been placed in operation
- Staff are competent
- Control covers 100% of the population



# Attributes of the “best” controls:

- **Invisible**
- **Automated**
- **Preventative**
- **Risk-based**



# IT General Controls

- **Access to Programs and Data**
- **Computer Operations**
- **Program Changes**
- **Program Development & Implementation**



# Access to Programs and Data Objective

To ensure that only authorized access is granted to programs and data upon authentication of a user's identity.



# Computer Operations Objective

To ensure that production systems are processed completely and accurately in accordance with management's objectives, and that processing problems are identified and resolved completely and accurately to maintain the integrity of financial data.



# Program Changes Objective

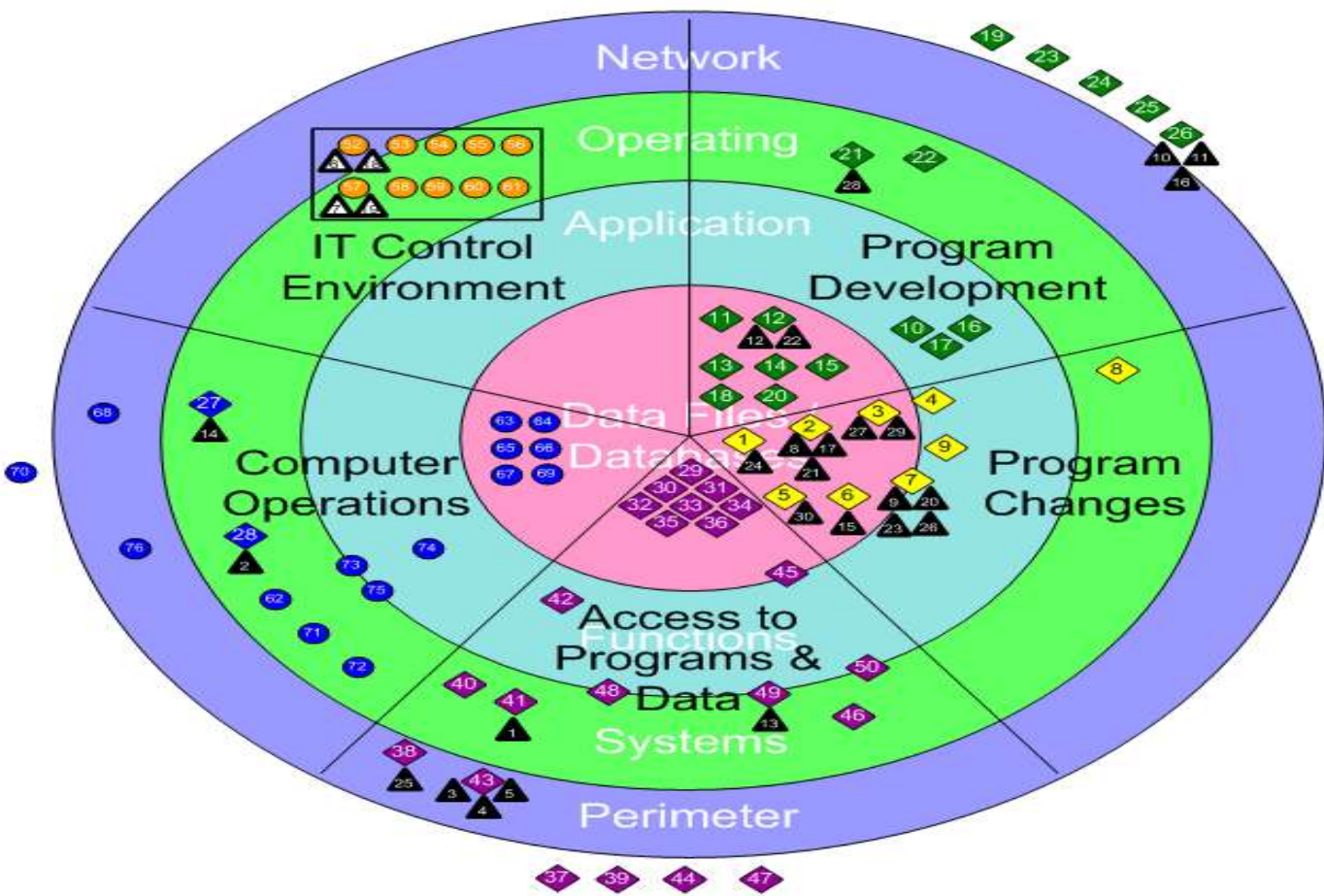
To ensure that changes to programs and related infrastructure components are requested, prioritized, performed, tested, and implemented in accordance with management's objectives.



# \* Program Development Objective

To ensure that systems are developed, configured, and implemented to achieve management's objectives.

# General Controls Review Key Controls, Control Activities, and Deficiencies



	Key Controls by Area	Control Activities by Area	Management Identified Deficiencies Key Controls
Change Management			
Development & Implementation			
Operations			
Security			
IT Control Environment			
			MSF Identified Deficiencies by Area
			Management Identified Deficiencies Non-key Controls
			Controls and Deficiencies identified cover all areas



FRAZER  
FROST, LLP  
Certified Public Accountants

Cody Griffin, CPA, CITP, CISA  
[cgriffin@frazerfrost.com](mailto:cgriffin@frazerfrost.com)  
(501) 537-7441