

# AMR Corporation

## Five Rules for Efficient IT Audits

Carolyn Gibson  
Managing Director, IT Audit  
American Airlines

October 9, 2008

# Learning Objectives

- Internal Audit best practices based on American Airlines' experience with Sarbanes Oxley audits
- How to manage the mixing of Sarbanes –Oxley assessments with traditional audits
- Successful methods and procedures that can be employed in Sarbanes-Oxley audits



## A little about AMR...

- Worlds largest scheduled airline
- Headquartered in Ft. Worth, Texas
- Currently serving 250 cities in 40 countries
- 85,000 employees



## On an average Day, American Airlines alone will...

- Transport about 270,000 passengers
- Receive more than 239,000 reservation calls
- Handle more than 300,000 pieces of luggage
- Fly about 3,300 flights



## Technology helps it happen...

- 250 critical systems
- 6 data centers
- 100-200 external parties providing:
  - Business Processes
  - System Operations
  - Application Development & Maintenance



What Could Possibly Go Wrong???



THE SUNSHINE  
WORLD EXCLUSIVES  
KEYS FOR

SAFE HARBOR  
IN A NASTY  
MARKET

WOW NEWS  
NEWS

# THE DAILY NEWS

www.dailynews.com

THE WORLD'S FAVORITE NEWSPAPER

- since 1879 -

## U.S. flight delays pegged to FAA computer woes



**Lorem ipsum** In libris graecis appetere mea. At vim odio lorem omnes, pri id iuvaret partiendo. Vivendo menandi et sed. Lorem volumus blandit cu has. Sit cu alia porro tuisset.

Ea pro natum invidunt repudiandae, his et facilisis vituperatoribus. Mei eu ubique altera senserit, con sul lenipit accusata has ne.

In libris graecis appetere mea. At vim odio lorem omnes, pri id iuvaret partiendo. Vivendo menandi et sed. Lorem volumus blandit cu has. Sit cu alia porro tuisset.

Ea pro natum invidunt repudiandae, his et facilisis vituperatoribus. Mei eu ubique altera senserit, con sul lenipit accusata has ne.

Ea pro natum invidunt



In libris graecis appetere mea. At vim odio lorem omnes, pri id iuvaret partiendo. Vivendo menandi et sed. Lorem volumus blandit cu has. Sit cu alia porro tuisset.

In libris graecis appetere mea. At vim odio lorem omnes, pri id iuvaret partiendo. Vivendo menandi et sed. Lorem volumus blandit cu has. Sit cu alia porro tuisset.

Ea pro natum invidunt repudiandae, his et facilisis vituperatoribus. Mei eu ubique altera senserit, con sul lenipit accusata has ne. Ignota verterem te nam, eu cibo causae menandi vim.

CLE HEADLINE

ppetere mea. At vim odio lorem aret partien do. Vivendo men andii et uis blandit cu has. Sit cu alia porro

int repudiandae, his et facilisis eu ubique altera senserit, con sul lenipit accusata has ne. Ignota verterem te nam, eu vim.

NEWS

PAPER - since 1879 -

CONCERNED  
CARDS

**Lorem ipsum** In libris graecis appetere mea. At vim odio lorem omnes, pri id iuvaret partiendo. Vivendo menandi et sed. Lorem volumus blandit cu has. Sit cu alia porro tuisset.

Ea pro natum invidunt repudiandae, his et facilisis vituperatoribus. Mei eu ubique altera senserit, con sul lenipit accusata has ne.

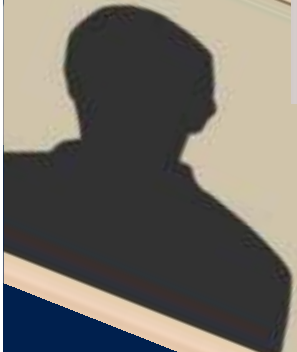
In libris graecis appetere mea. At vim odio lorem omnes, pri id iuvaret partiendo. Vivendo menandi et sed. Lorem volumus blandit cu has. Sit cu alia porro tuisset.

Ea pro natum invidunt repudiandae, his et facilisis vituperatoribus. Mei eu ubique altera senserit, con sul lenipit accusata has ne.

Ea pro natum invidunt

London  
crippled

outage  
Lorem ipsum  
In libris graecis appetere mea. At vim odio lorem omnes, pri id iuvaret partiendo. Vivendo menandi et sed. Lorem volumus blandit cu has. Sit cu alia porro tuisset.



## And then what ?

- Negative impact to operations
- Loss of customer confidence
- Compromised reputation
- Worried shareholders
- Going venture concern

# The IT Audit Challenge...



## The number of systems in scope continues to increase but headcount remains virtually flat...

	2003	2004	2005	2006	2007	2008
Number of GCRs	6	19	29	34	60	66
Average Headcount (FTE)	5.4	5.8	6.2	5.5	5.5	5.75
Reviews per FTE	1.1	3.3	4.7	6.2	10.9	11.5



Increase efficiency without increasing risks?



## Systems may be high risk for multiple reasons...

	SOX	PCI	Safe Harbor	New Development	Operation Critical
Customer Facing Websites		✓	✓	✓	✓
In-Flight Applications		✓	✓	✓	
Reservations	✓	✓	✓		✓
Fueling	✓				✓
Payroll	✓		✓		✓
Frequent Flyer	✓	✓	✓		✓



**Although the forces driving audit scope are different, the basic risk factors are the same so testing can be leveraged for multiple constituencies...**

	SOX	PCI	Safe Harbor	New Development	Operation Critical
Physical Controls	✓	✓	✓	✓	✓
Operations/Backup	✓	✓	✓	✓	✓
Network Security	✓	✓	✓	✓	✓
O/S Layer Change & Access	✓	✓	✓	✓	✓
D/B Layer Change & Access	✓	✓	✓	✓	✓
App Layer Change & Access	✓	✓	✓	✓	✓
DR/BCP				✓	✓



# Rule #1

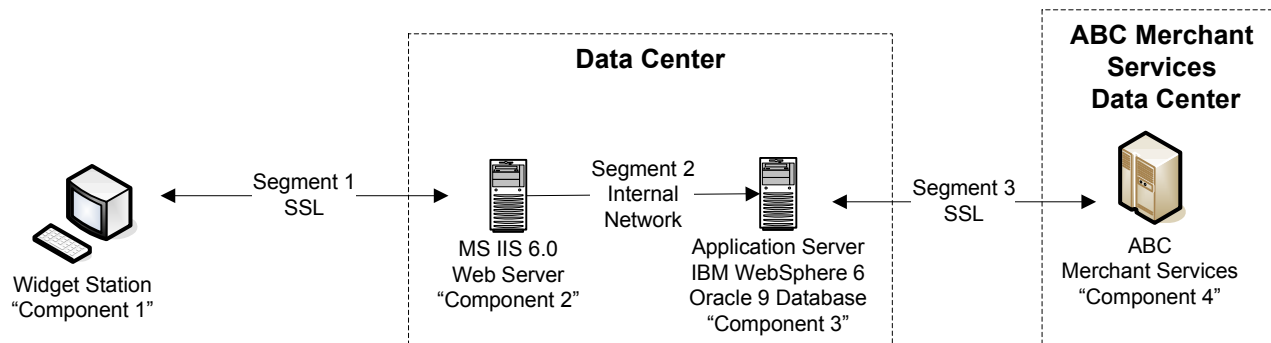
## Audit Systems ONCE



# Our audit program begins with tests of general controls that are applicable in all environments...

## Architectural Component Summary

**EXAMPLE - Widget Kiosk** - When a customer swipes their payment card the kiosk will read the data from the card magnetic stripe to obtain the cardholder data for the purpose of purchasing various passenger services.



1. – Component 1: The card swipe keyboard, or the Widget application permits credit card data entry
2. – Segment 1: Encrypted SSL session
3. – Component 2: MS IIS 6.0 Web Server
4. – Segment 2: Internal network
5. – Component 3: Widget IBM WebSphere application server and Oracle Database
6. – Segment 3: The Widget application server establishes an encrypted SSL connection for the duration of the credit card authorization
7. – Component 4: PCI approved merchant service

Summary: The last 4 digits of a credit card are stored in the Oracle table "CO2", in the "CC" field during authorization



# Then it's augmented depending on the specific risks...

**Data Storage**  
**PCI – 3.1, 3.2, 3.3, 3.4, 3.5,**  
**3.6**

PCI Components	Description			
PED	As of January 2008, the Industry requires an authentication (e.g. PIN, Identification Number, keypad, OSR, etc. The Standard is concerned with the management, processing, and storage of PIN data during only payment card transactions at attended and unattended terminals.			
Point of Sale Receipt	If system is classified as a cardholder, obtain a receipt from the customer, obtain a receipt from the customer.			
Data Display	Does this component display or print any cardholder data?	The last 4 digits of the card are printed on the receipt.		
Data Storage PCI - 3.1, 3.2, 3.3, 3.4, 3.5, 3.6	Does this component store any cardholder data, even temporarily (e.g. cache. Logs, databases, backup media)?	No each transaction is performed between the application server and the host.		
Data Transmission	Does this component transmit any cardholder data to another architecture component, via email, or direct connect to another network?	Data is captured through this POS to the application server. See appropriate section in the Component Segment table.		
Data Retention Awareness	Are account users on this component aware of AMR data retention policies?	Yes		
Audit Log File Access PCI - 10.1	Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	Provide process and screen capture that audit trails are enabled and active, including for any connected wireless networks.		



## Benefits of Rule #1...

→ Minimize client contact



→ Reduce impact to daily operations



→ One report contains all pertinent issues



# Rule #2

## Don't Over Test



# EXAMPLE: Revenue Accounting System...

- 42 Subsystems
- Relevant to 54 significant accounting processes
- 19 controls
- 300+ hours testing IT controls

## Other Relevant Factors:

- Legacy system with limited or no changes
- General IT controls tested annually since 2004 with no errors detected
- Extensive ticket transaction testing annually



## Conclusions:





- System was too complex to reduce ticket testing
- Ticket testing proved reliability of subsystems
- Application change controls were strong and static

## New Testing Approach:

- Continue ticket transaction testing
- Document application changes since 2006
  - No changes in 2007, or YTD 2008
- Rely on application change control testing
- Test one subsystem transaction



## Benefits of Rule #2...

- Reduced testing time 
- Didn't increase risk of undetected issues 
- Reduced impact to audit client and operations 
- Auditor hours can be redirected to other areas 



# Rule #3

## Rely on Other Professionals!!!



## EXAMPLE: Data Center Reviews...

- 6 data centers
- Operated by third parties
- Critical to business continuity and system security
- Testing consumed 300-500 hours annually

### Other Relevant Factors:

- Established centers with limited or no changes
- Tested annually since 2004
- Type II SAS 70s performed by Big 4 firm



## Conclusion:





- Physical controls are strong and not subject to sampling
- Operational controls (e.g. job scheduling, system capacity monitoring) were strong
- Issues would be evident in daily operations and supported by a mature problem management process
- O/S controls are tested on a sample basis

## New Testing Approach:

- Rely on SAS 70 for physical and operational controls
- Independently test O/S, D/B and Application controls



## Benefits of Rule #3...

- Reduced testing time 
- Didn't increase risk of undetected issues 
- Reduced impact to service provider and operations 
- Auditor hours can be redirected to other areas 



# Rule #4

## Reduce GCR Testing



## EXAMPLE: Flight Operating Systems

- Year 1 SOX: 300-400 manual and IT controls documented
- Emphasis on defining “all” key IT or IT dependent controls
- General controls testing performed on all relevant systems
- The theory: Strong general controls = less manual testing

### Other Relevant Factors:

- Application controls tested since 2004 with no significant issues
- General controls were common across mainframe applications
- General controls were strong and static



## Conclusion:





- Strong general controls ≠ less manual testing
- General controls were being tested via other mainframe applications

## New Testing Approach:

- Don't perform general controls testing on Flight Operating System



## Benefits of Rule #4...

- Reduced testing time 
- Didn't increase risk of undetected issues 
- Reduced impact to audit client and operations 
- Auditor hours can be redirected to other areas 



# Rule #5

## Test All Year



## EXAMPLE: Mainframe User Access Control

- Year 1 SOX: 25 transactions spanning 10 calendar months
  - Drove large workload 4Q
- Consistent process across environment
- Process executed by third party service provider

### Other Relevant Factors:

- Sample size is static (assuming no deficiencies)
- Testing methodology is static
- Service provider/customer relationship forces segregation of duties



## Conclusion:




- Testing could be performed in small samples throughout the year

## New Testing Approach:

- Move to a continuous auditing model
- Sample 5 transactions per quarter or 100% whichever is less



## Benefits of Rule #5...

- Didn't increase risk of undetected issues 
- Reduced impact to audit client and operations 
- Issues are detected earlier in the year 



## Last Thoughts...

- SAMPLE across environments
  - Provisioning systems
  - Mainframe change control
- Alter testing approach based on previous results
- Scrub key controls
- Design efficient tests that vouch for multiple controls
  - Focus efforts on tests that reduce manual testing
- Resource continuity
- Perform an annual IT Audit program review and refresh if appropriate



# Information Retrieval Exercise AKA: TEST...

## Rule #1

→ Audit Systems ONCE

## Rule #2

→ Don't Over Test

## Rule #3

→ Rely on Other Professionals

## Rule #4

→ Reduce GCR Testing

## Rule #5

→ Test All Year



# Questions...

