

April 24, 2008

Andrew Pinnero, Director IT
Buddy Arriola, Manager IT

Collaborative Approaches in Identifying, Assessing and Protecting Data Assets



Agenda

- Understanding Business Process Risk and IT Risk
- Identifying Management's Risk Appetite
- Independent Assessment of IT Risk
- Now What Do You Do? Case Study
- Questions

How do We Measure Data Risk?

- There are numerous methods to understanding IT based data risk...here are a few:
 - Technical approach (Pen Testing, Internal Scans, Procedural Reviews)
 - Business Process approach – Understand risks embedded in the business processes and applications supporting the business process

Connective Risk – An Overview

- Ensuring that both IT and the business stakeholders have a common understanding of IT risk at various data points
- IT's impact on basic business processes
- IT Risk - Possibility of loss as a result of inappropriate utilization of IT resources
- IT Controls – Physical and logical mechanisms used to mitigate system relevant risks

Connective Risk & Four IT Related Process Risk

- Financial Risk
- Strategic Risk
- Operational Risk
- Compliance Risk

Four IT Related Process Risks

- Financial Risk - As most systems potentially have some effect on your Company's financial controls and customer services, the level and likelihood of such an effect needs to be considered.
- Strategic Risk – IT Systems may have a direct strategic effect on your Company (especially the manner in which customer data is used to move the company forward).

Four IT Related Process Risks (cont)

- Operational Risk- Most system risk stems from this area as IT is designed to affect the manner in which and the effectiveness by which your Company conducts its day to day business.
- Compliance Risk -Systems can have a direct effect on how your Company complies with statutory obligations.

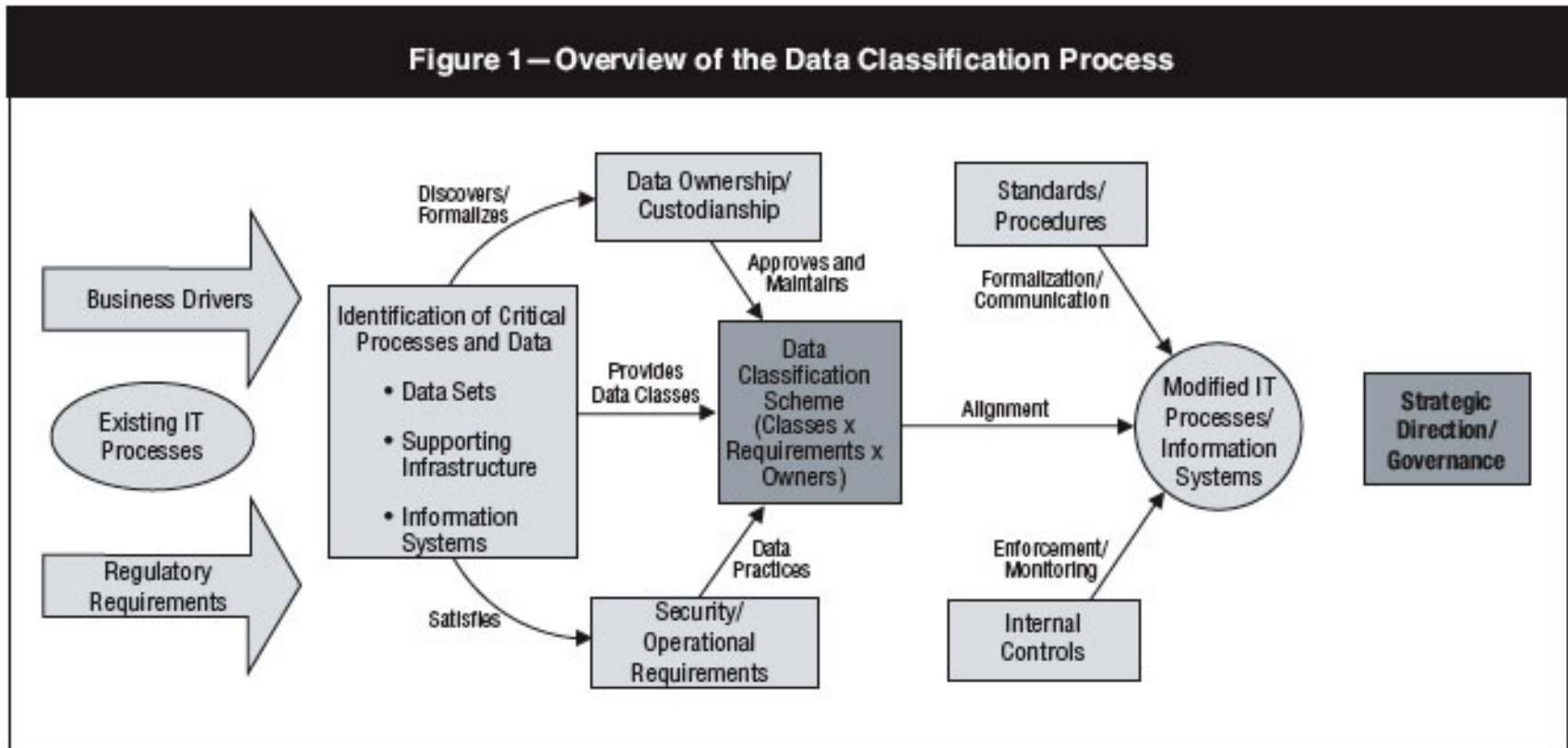
Understanding Enterprise Risk Tolerance and Risk Appetite

- Corporate culture weighs heavily on how management reacts to and manages data risk
- IT Management’s “risk appetite” is often a reflection of “C” level management attitude towards risk
- Some companies have/had high risk appetite
 - WorldCom / Enron
 - IT management reflected CEO’s risk appetite by ignoring controls that mitigate or reduce unethical behavior

“It is all about the data, Stupid!”

- The stakeholders need to know how IT protects their core data given formal security classifications
- IT needs to know which data to protect and use classification guidelines as the basis by which to configure application, db, OS and network security

Data Classification: COBIT



Source: WWW.ISACA.ORG

Data Classification

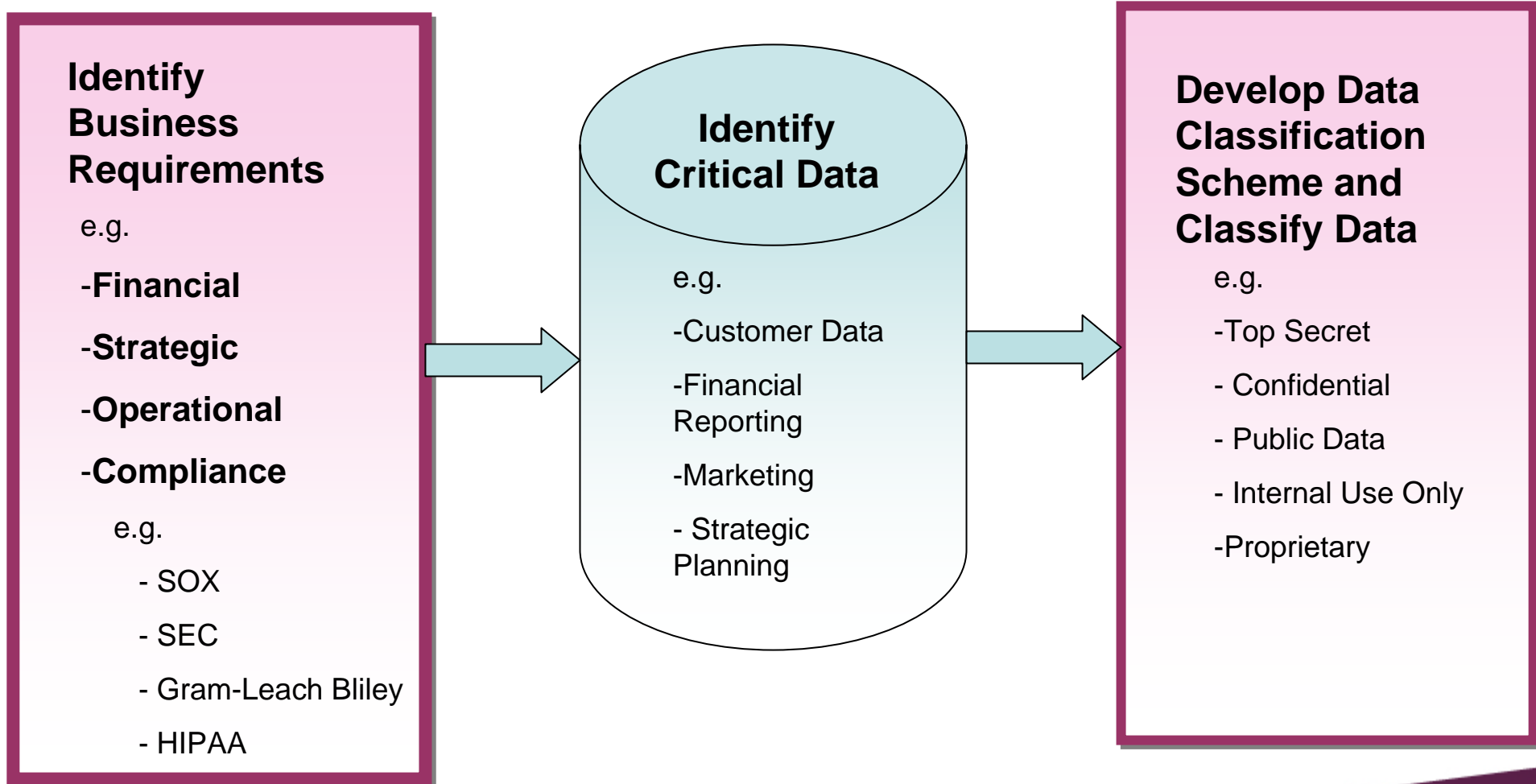
Step 1: Identify all critical data, data owners, systems and processes supporting these data, and existing data controls

Step 2: Determine business and regulatory requirements

Step 3: Develop data classification standards based on requirements

Step 4: Classify data

Data Classification



Data Classification :

Regulatory Requirements

- **SEC rule 17a-4** at least 6 year retention period, the first two in easily accessible place
- **SEC rule 2-06(a)** Audit & Reviews, 7 year retention period
- **HIPAA** – Data Retention, confidentiality, integrity, and availability of patient info; medical records, 6 year-, and 2 year-retention period after death of a patient Penalty: up to \$250,000 fine and 10 years imprisonment
- **Gramm-Leach-Bliley Act** Penalty: - Data integrity and privacy of personal consumer information Penalty: criminal prosecution, fine and up to 5 years imprisonment
- **FDA:** (Manufacturing, Processing, and Packing information)
 - Drugs – 3 years after distribution
 - Bio Products – 5 years after end of manufacturing
 - Food – 2 years after release

Data Classification Scheme

- Top Secret – Exposure could cause serious damage
 - Example: Pending mergers/acquisitions
 - System: e Mail/ Local network drive
- Confidential – Could seriously impede the Company's daily routines and is considered critical for ongoing operations
 - Example: Membership data, salaries, digital signatures, medical information
 - System: Membership database/CMS/payroll applications/various HR db's
- Public Data - Information in the public domain
 - annual reports, press releases
 - System: Website/Intranet

Data Classification Scheme (continued)

- Internal Use Only – Should be protected but if lost would not impede the reputation of the Company
 - Meeting memos, training materials, status reports,
 - System: email server/Project management tools
- Proprietary – Designs and specs that define the way in which the Company operates
 - Example: AP/AR procedures, run books, survey designs
 - System: Local Network drives/ embedded in source code

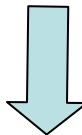
Data Management



Classified Data

e.g.

- Subscriptions (confidential)
- Financial Reporting (Confidential)
- Marketing (Proprietary, Internal use)
- Strategic Planning (Top Secret)

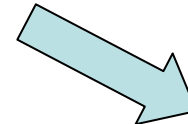
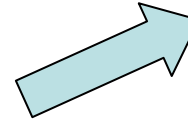


Change Management

e.g. Addition, Deletion, Modification of key data subject to Change Management Policy & Procedures

Access Controls

e.g. role based access for key applications and data



Data Handling

e.g. Encrypt electronic transmission of Confidential Data;

Data Retention

e.g. Financial Report, SOX 7 year retention

Backup

e.g. Full Daily backup for all Key systems and data

Storage

e.g. Encrypt and password protect Confidential Data, stored on laptops and portable media

Management's Self Assessment on How They View Data

- “Take a Step Back” and Consider:
 - What is Management's IT Risk appetite and how do you measure it? - For example what attributes does management use to measure the tolerance and management of excess IT risk
 - What is Management's Approach to Monitor current IT Risk
 - How is the Enterprise Positioned to address IT Risks from Emerging Technologies (i.e. Cloud computing and Social Networking)

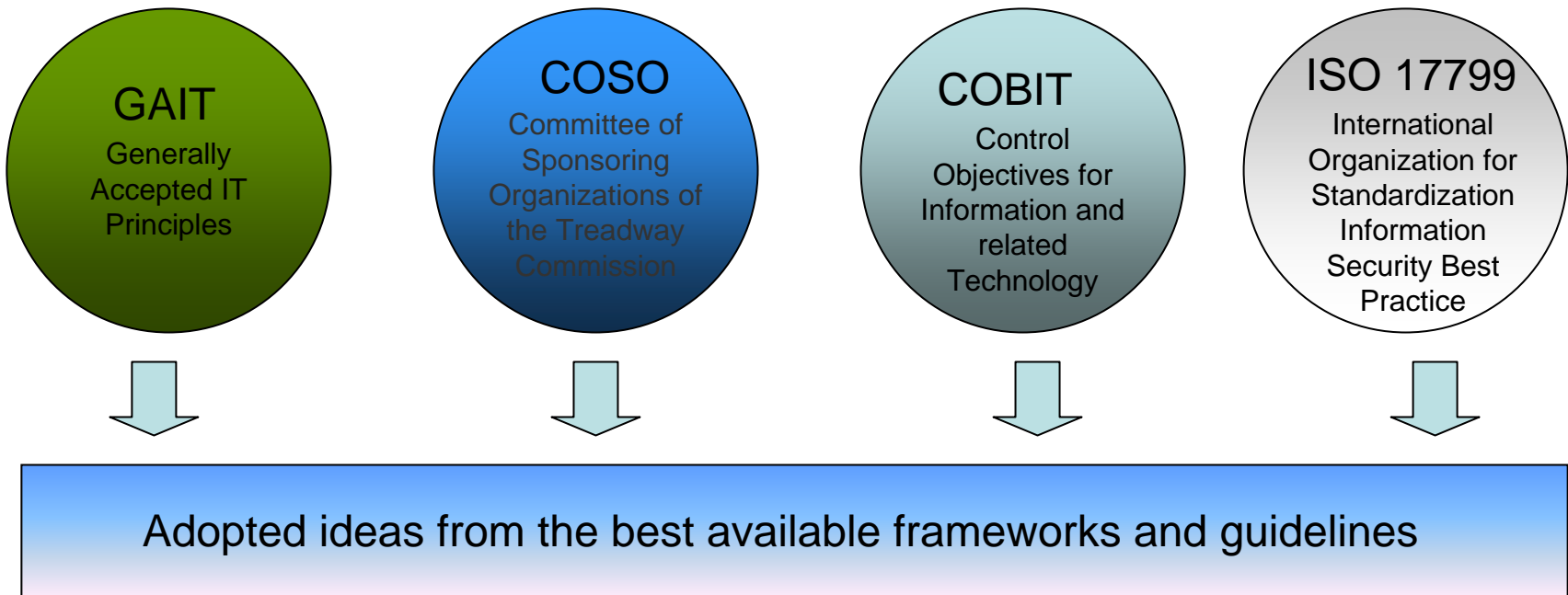
Seek out Objective Critique of Management's Risk Appetite

- Management should seek out objective sources to opine on their understanding and management of IT risk
- Engage with Internal Audit, Compliance Officer etc. to gain feedback
- Ensure assessment addresses all components of IT data risk

Perform an Independent Review

- Measure “perceived” risk (based on management’s risk appetite and data classification) to an actual “independent” diagnostic of the general IT control risk posture as it relates to data.
 - IT Policies/Strategy/Procedures
 - SDLC/Change Control
 - DRP/Backup/Media Transfer
 - Integrations
 - DB/OS Security
 - Network Security
 - Application Security

Frameworks used for an Assessment



Case Study:

XYZ Insurance Company

Company Profile:

- Mid-sized company
- 250 FTE's
- 25 person IT shop
- IT Reports to CFO
- Management has various projects going on and their risk appetite varies with each project and/or piece of data

Case Study:

XYZ Insurance Company

Part I.

MANAGEMENT

SELF-RISK ASSESSMENT

Case Study:

XYZ Insurance Company

Assumptions:

- Data universe has been established by management
- Identified the following as key data and to audit these periodically:
 - Financial
 - Strategic
 - Operational
 - Compliance
- Management gathered information through inquiries and interviews with key personnel

Case Study: Measuring Management's Risk Appetite Can be Subjective

FINANCIAL	RISK APPETITE
<ul style="list-style-type: none">• Financial applications are deemed critical in mitigating fraud and disclosure errors	Low
<ul style="list-style-type: none">• Interfaces are regularly monitored and data reconciled	Low
<ul style="list-style-type: none">• Web based Payroll portal does not use encrypted sessions and users from IT have access to the system	
<ul style="list-style-type: none">• Financial applications are deemed less critical (and are not secured) in mitigating fraud as management relies on substantive controls	

Case Study: Measuring Management's Risk Appetite Can be Subjective (cont)

STRATEGIC	RISK APPETITE
<ul style="list-style-type: none">• Customer data is a strategic necessity and protected via IT controls	Low
<ul style="list-style-type: none">• Management does not see the need to implement an AMS (Customer Database System) that IT would need to help secure customer data	
<ul style="list-style-type: none">• Customer data is generally not used to position the company for future growth	

Case Study: Measuring Management's Risk Appetite Can be Subjective (cont)

OPERATIONAL	RISK APPETITE
<ul style="list-style-type: none">• Databases and networks supporting key systems should be constantly monitored for unauthorized access	Low
<ul style="list-style-type: none">• Outsourcing to a VPS based host only after extensive review of vendor SAS70 and SLA/NDA	Low
<ul style="list-style-type: none">• Backup media is sent offsite to a third party vendor that has weak security practices	
<ul style="list-style-type: none">• IT operations should just “keep the lights on” and let management worry about risk	

Case Study: Measuring Management's Risk Appetite Can be Subjective (cont)

COMPLIANCE RISK	RISK APPETITE
<ul style="list-style-type: none"> • Data security standards match or exceed competitors 	Low
<ul style="list-style-type: none"> • Management has implemented a formal CAN-SPAM policy to address regulatory fines 	Low
<ul style="list-style-type: none"> • Our company is not regulated so risk assessments are an unnecessary burden 	
<ul style="list-style-type: none"> • Software copies are regularly distributed throughout the company (BSA announces \$1 Million reward for whistleblowers during summer '07). 	

Case Study:

XYZ Insurance Company

Part II.

INDEPENDENT RISK ASSESSMENT

Case Study:

XYZ Insurance Company

Assumptions:

- Internal Audit conducted general IT controls review in the prior year and has familiarity with the company's IT general and application based controls
- Stakeholders have bought into the concept of securing various types of data

Case Study: The Business Process Based IT Risk Assessment

Process	IT System	Resident Data w/(Risk Type) (Risk Adversity)				
		TS	Conf	Prop	Intern	Public
Subscriptions	Customer database or AMS (Homegrown)		Customer data (S,O) (H,H)			
Financial Reporting	Epicore (Fin Reporting)		Fin Rpt data (F) (H)			
	Spreadsheets on Drive E:\Fin\Docs\2008 Budg		Budget.xls (S,F) (L,L)			
Marketing	MS Project on Drive E:\Marketing\NewProj				New Project (S) (L,L)	
Strategic Planning	CEO Exec Assistant Drive E:\CEO\Assist\	LT_Strat.doc (S,O) (L,L)				

Case Study: Understand IT System Risk Impact on Business Processes

- Outsourced – Vendor hosts and maintains
 - Outsourced controls may increase security risk
 - Other companies may be on same physical server
 - Trusted domains
- Home grown – Internally developed Systems
 - Programmers know how to circumvent controls
 - Unauthorized changes could be migrated to Prod
- 3rd party
 - Security in smaller applications may not be robust
 - Limitations on ability to monitor application activity
- Desktop Applications
- Web Based Systems
- Networked Systems

Case Study: Measuring IT System Controls

Management has identified “confidential data” within the “Homegrown System” Customer DB... Ask:	Customer DB	Risk Rank (10=H)
Do staff programmers have access to live data?	Y	10
Are changes Properly tested by end users?	Y –w/exceptions	2
Does management perform a detailed “confidential data” entitlement review on a periodic basis?	N	6
Does the DB challenge users with a PW?	Y	2
Are users locked out after x amount of attempts at a failed login?	N	7
Total IT System Score		27/50

Case Study: Assessment Score Breakdown

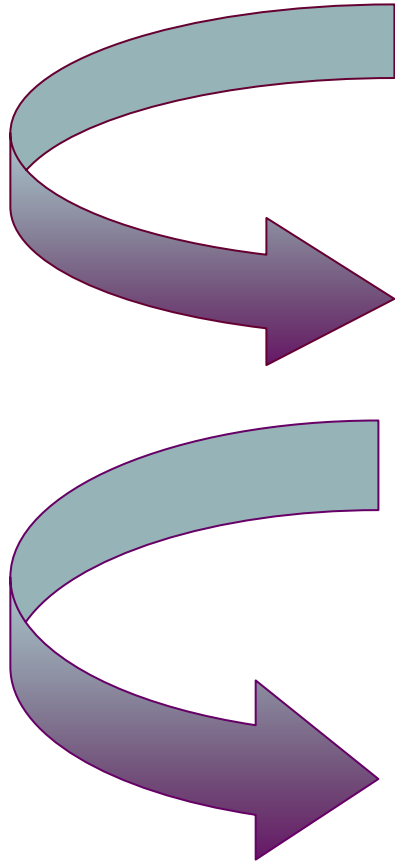
Process	Application/ Assessor	Target Data	TD Score	Strat	Fin	Ops	Comp
Subscriptions	Customer DB		27				
		Customer Data (Name/Address from IA) (H=4, L=1)		4	1	4	1
		Management's Risk Appetite Score {H=1/L=2}		2	1	2	2
		Classification {Confidential}		4	4	4	4
		Totals	27	(4*4*2) =32	4	32	8

Key: Classification Score (TS = 5/ Conf=4/ Prop=3/ Internal Use=2/ Public=1)

Case Study: Summary Assessment Scores by Target Data

Process	Application/ Assessor	Target Data	TD Score	Strat	Fin	Ops	Comp
Subscriptions	Customer DB	Customer data	27	32	4	32	8
Financial Reporting	Epicore	Quarterly and Year end financial statement	18	4	20	16	20
Finance	Spreadsheets on Drive	Payroll data	40	4	20	8	8
Finance	Spreadsheets on Drive	E:\Fin\Docs\2008 Budg	20	16	4	4	10
Marketing	MS Project on Drive E:\Marketing\New Proj	Marketing data	38	16	16	4	10
Strategic Planning	CEO Exec Assistant Drive E:\CEO\Assist\	Exec Assistant data	36	20	4	10	4

Summary



**Collaborative
Business/IT approach**



Remediation



Improved Data Security



THANK YOU!

Andrew Pinnero:
apinnero@verisconsulting.com

Buddy Arriola:
barriola@verisconsulting.com