# *Industry Trends – An Introduction to Security Breach Prevention, BYOD, & ERP System Implementation*

The Central Florida Chapter of The Florida Government Finance Officers Association
2/7/2014

K. Adam Glover, CISA

Cherry Bekaert LLP
Your guide forward

# *Key Points Agenda*

- Security Breach Prevention Overview
- Introduction to BYOD, MDM, & ERP
- Mobile & Industry Trends
- BYOD Policy & MDM Characteristics
- ERP Requirements & Characteristics
- Managing the Implementation Process
- Common Pitfalls of an ERP Implementation

Cherry Bekaert LLP
Your guide forward

# *What do all these acronyms mean?*

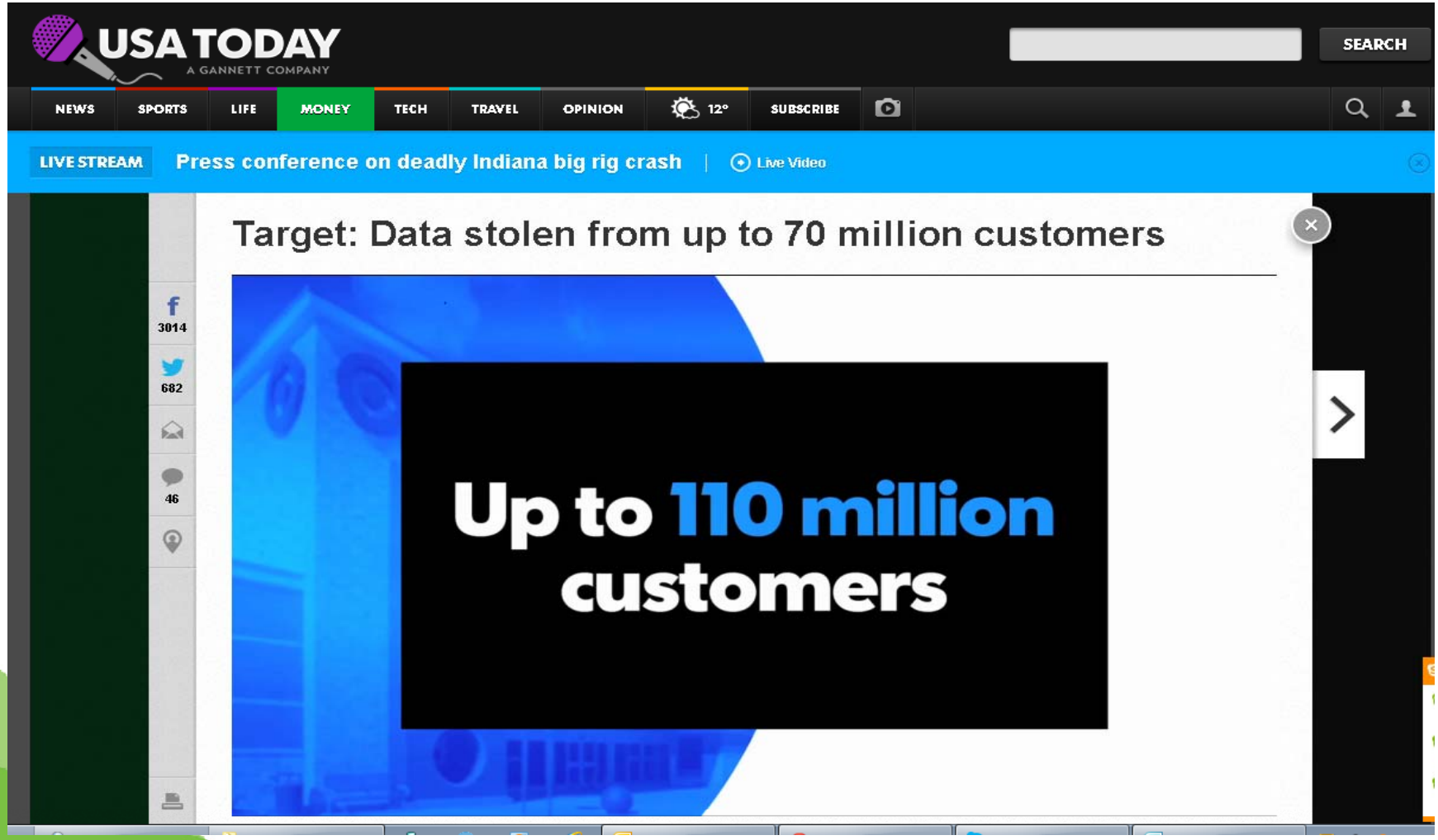
- BYOD (bring your own device) and BYOT (bring your own technology)
  - Main concern: (Technical) security issue
- MDM (mobile device management)
  - Used to secure, monitor, manage, and support deployed mobile devices
  - Applies to both company and employee owned devices
- ERP (Enterprise Resource Planning) Software
  - The Most Important Thing to Remember: You can increase the likelihood of success through proper *planning and documentation*

# *Security Breach Prevention*

Cherry Bekaert LLP

*Your guide forward*

# *Security Breach Example #1*




Cherry Bekaert LLP
Your guide forward

# *Security Breach Example #2*

FOX NEWS .com Fair & Balanced

Search

Listen to Fox News Radio Live >

ON AIR NOW >

9a et America's Newsroom

WATCH LIVE

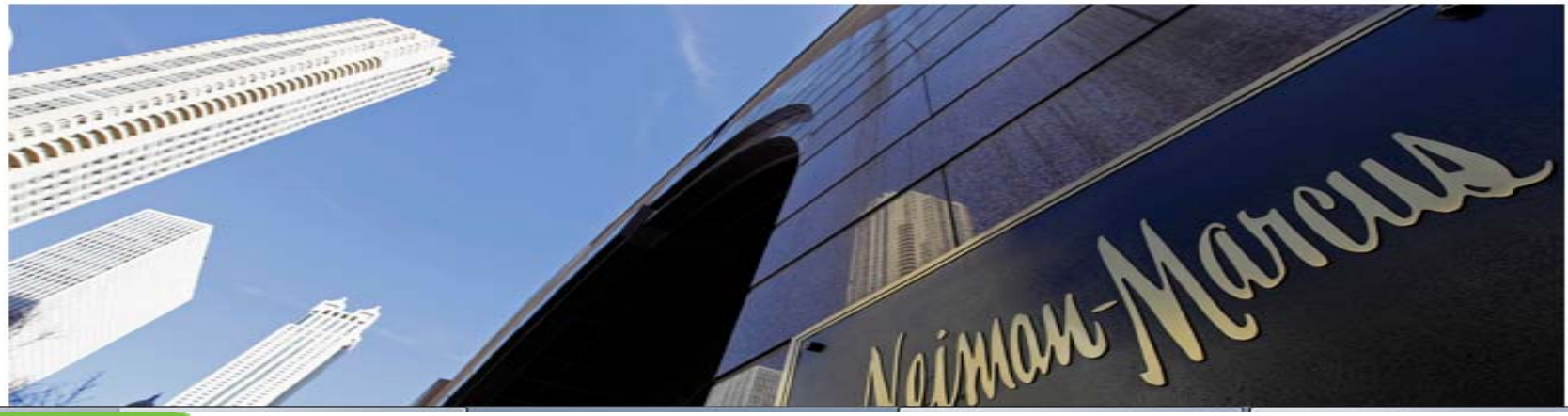
Home | Video | Politics | U.S. | Opinion | Entertainment | Tech | Science | Health | Travel



Home | Gadgets | CES 2014 | Computers | Military Tech | Smartphones | Video Games | Slideshows

## Neiman Marcus says security breach may affect up to 1.1 million cards

*Published January 24, 2014 / Associated Press*




Cherry Bekaert LLP

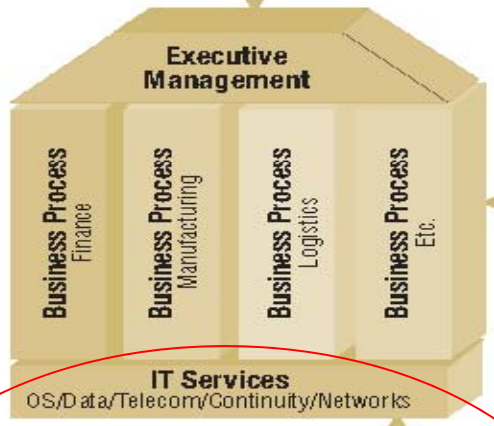
Your guide forward

# *Overview of IT General Controls*

## Figure 2—Common Elements of Organizations

**Entity-level Controls**
Entity-level controls set the tone and culture of the organization. IT entity-level controls are part of a company's overall control environment.

Controls include:
- Strategies and plans
- Policies and procedures
- Risk assessment activities
- Training and education
- Quality assurance
- Internal audit




**Application Controls**
Controls embedded within business process applications directly support financial control objectives. Such controls can be found in most financial applications including large systems such as SAP and Oracle as well as smaller OTS systems such as ACCPAC.

Control objectives/assertions include:
- Completeness
- Accuracy
- Existence/authorization
- Presentation/disclosure

**IT General Controls**
Controls embedded within IT processes that provide a reliable operating environment and support the effective operation of application controls

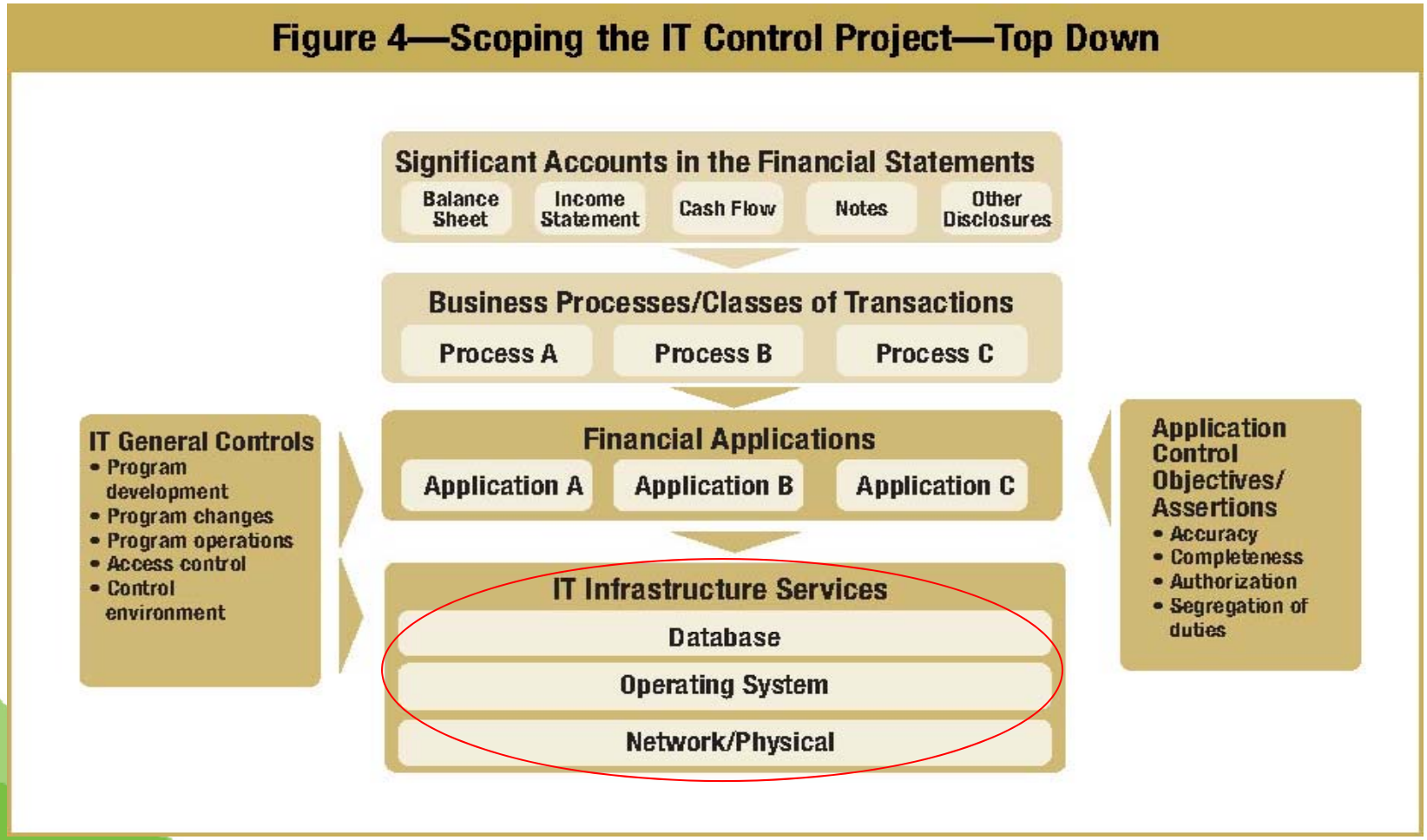
Controls include:
- Program development
- Program changes
- Access to programs and data
- Computer operations

Cherry Bekaert LLP
Your guide forward

# *Overview of IT Controls in an Audit Cont.*

- With widespread reliance on IT systems, controls are needed over such systems, large and small.
- IT General Controls (ITGC) are needed to support the functioning of application controls, and both are needed to support accurate information processing and integrity of the resulting information used to manage, govern, and report on the organization.
- As automated application controls increasingly replace manual controls, IT general controls are becoming more important.

# *Linkage of ITGC to Financial Statement Accounts*




Cherry Bekaert LLP
Your guide forward

# *Access & Security*

- Control Objective:
  - Physical security and access to programs and data are appropriately controlled to prevent unauthorized use, disclosure, modification, damage, or loss of data.

- What's the ***risk***?
  - Without effective logical and physical controls in place financial data could be lost, changed, or used inappropriately and the accuracy and integrity of financial information produced by the system could be compromised.

# *Access Control Activities*

- Strong Password & Account Lockout Security Policies
- Account Creation, Maintenance, and Termination
- Segregation of Duties
- Periodic Review of Access
- Encryption – hard drive, data & removable media (USB drives)
- Ensure you have good Network & System Health Monitoring in place (firewall monitoring, vulnerability assessments, etc.)
- Service Organization Evaluations (SSAE 16/SOC 1 Reports, SOC 2 & SOC 3 Reports, PCI Compliance Certificates, etc.)
- Review the PCI Self-Assessment Questionnaire which can be found here: https://www.pcisecuritystandards.org/merchants/self_assessment_form.php

Cherry Bekaert LLP
Your guide forward

# *Introduction to BYOD & MDM*

Cherry Bekaert LLP

*Your guide forward*

# *Devices to Include*

- Laptops
- Cell and Smart Phones
- Tablets
- E-Readers
- Mobile Hotspots
- Mobile Storage
- Etc.

**B.Y.O.D.**

**(Bring Your Own Device)**

Cherry Bekaert LLP

*Your guide forward*

# *Mobile Trends Research Part I*

- Smartphones
  - 70% belong to users & are bought by users
  - 12% are chosen from an approved list & using a corporate discount
  - 16% are corporate-issued
  - 3% shared the cost
  - 5% paid for by their companies
  - By 2016 350 million employees will use smartphones
  - By 2016 38% of companies expect to stop providing devices to workers
  - By 2017 50% of all companies will require employees to bring their own smartphones

Cherry Bekaert LLP
Your guide forward

# *Mobile Trends Research Part II*

- Tablets
  - 65% belong to users
  - 15% are chosen from an approved list
  - 16% are corporate issued
  - 58% bought their own
  - 17% corporate discount
  - 7% shared the cost
  - 18% paid for by their companies

Cherry Bekaert LLP
Your guide forward

# *Industry Trends*

- Kaspersky reports 33% of companies allow unrestricted access to corporate applications from smartphones
- 38% of companies employ restrictions on mobile use
- 20% have complete BYOD ban
- 23% loss of business data through loss of mobile device
- By 2015 the number of employees using mobile applications will double
- U.S. Companies are twice as likely to allow BYOD as Europe

Cherry Bekaert LLP
Your guide forward

# *BYOD Policy Concerns*

- Supported devices
- Device ownership
- Expectation of privacy
- Installing apps
- Jailbreaking / rooting
- Incident response
- Regulatory compliance
- Data restrictions for smartphone users
- Termination procedures / device recovery


Cherry Bekaert LLP
Your guide forward

# *Elements of a Sound BYOD Policy Part I*

- Require a signed agreement
- Require device enrollment
- Eligibility requirement and approval processes
- Disclaimer for personal loss
- Employee risk and responsibilities
- Throw away devices for travel to high risk areas
- Explicitly state what rights the company retains to data on personal devices
- Explicitly state what data the employee is required to remove upon separation
- Device support limitations
- Applications and data access limitations

Cherry Bekaert LLP
Your guide forward

# *Elements of a Sound BYOD Policy Part II*

- Required security features like:
  - Authentication
  - Automatic timeouts
  - No jailbreaking or rooting
  - Disable capabilities (removable storage, camera, BlueTooth, IR, etc…)
  - Wipe policies
- Implement policies stating that the company retains the right to:
  - Track employee usage, location, or other information
  - Document the right of the company to share that data with third parties
- Timing to report lost/stolen device
- Decommissioning device
- Policy violations

Cherry Bekaert LLP
Your guide forward

# *Items to Update Relating to BYOD*

- Policies to Update:
  - Acceptable Use Policy
  - Remote Access & Mobile Computing
  - Asset Management
  - Security Incident Response

- Security Awareness Training
  - Update training to include security overview of BOYD strategy & policy updates

# *Typical MDM Functionality*

- Includes over-the-air distribution of:
  - Applications
  - Data
  - Configuration settings
- For all types of mobile devices, including:
  - Mobile phones
  - Smartphones
  - Tablet computers
  - Ruggedized mobile computers
  - Mobile printers

# *MDM Requirements*
# *Part I*

- Separation of duties
- Establishing your requirements for company-owned devices
  - Screen locking
  - Password length and change times
  - Internet filtering
  - Application restrictions
  - Remote access to the company network
  - Encryption
  - Reporting into the MDM
  - Alerting
  - Pre-registration before device delivery

Cherry Bekaert LLP
Your guide forward

# *MDM Requirements Part II*

- The same requirements should apply to non-company owned devices
- Establish rules for who can have a non-company owned device connection
  - Staff who are approved to use a company-owned device but choose to use their own
  - Level of approval should be higher than the staff's manager
  - Pre-registration and not automated
  - What can be accessed that is different from a company-owned device
  - Stewardship agreement
  - Liability / cost for device plans or additional costs to company
- MDM group establishment
  - Company-owned versus Non-company-owned
  - Employee versus third party
  - Integrated into LDAP
- Authentication
  - Single-sign on
  - Multi-factor

# *MDM Requirements*
# *Part III*

- Mobile Applications
  - Costs of installed applications
  - Standardized list of mobile applications
- What mobile devices do you want to support
  - Mobile phones
  - Smartphones
  - Tablet computers
  - Ruggedized mobile computers
  - Mobile printers
- Standard for
  - Make / Vendor
  - Model
  - Operating system version(s)

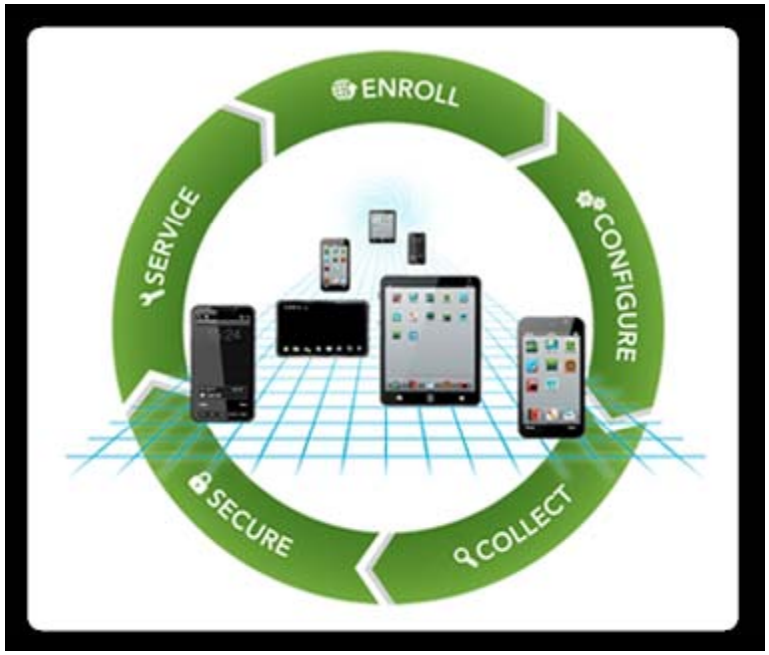
# *Additional MDM Considerations*

- Host in the cloud or onsite?
- Do you want to permit tunneling?
- Application controls
- Secure storage
- Authentication
- Access via provider or hotspot or corporate network
- Internally developed mobile application integration
- Application black/white listing
- Device wiping – profile or whole device

Cherry Bekaert LLP
Your guide forward

# *MDM Solutions*

- Good Technology
- AirWatch
- BoxTone
- Casper (JAMF Software)
- Juniper Networks
- MobileIron
- RIM (BlackBerry)
- Sophos




Cherry Bekaert LLP
Your guide forward

# *Key Points to Remember*

- Create a policy prior to selecting an MDM solution
- Establish standards for allowed devices
- Take an inventory of devices already accessing the network
- Certify simple device enrollment
- Configure devices over the air
- Maintain a self service kiosk
- Create clear definitions between personal and corporate data
- Protect those definitions between personal and corporate data
- Manage data usage
- Monitor the system and audit periodically

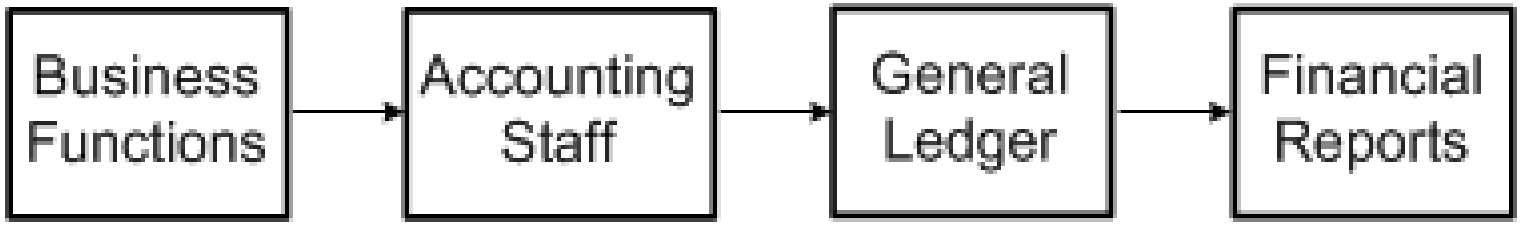
# *ERP System Implementation*

Cherry Bekaert LLP

*Your guide forward*

# *What is an ERP System vs. an Accounting System?*

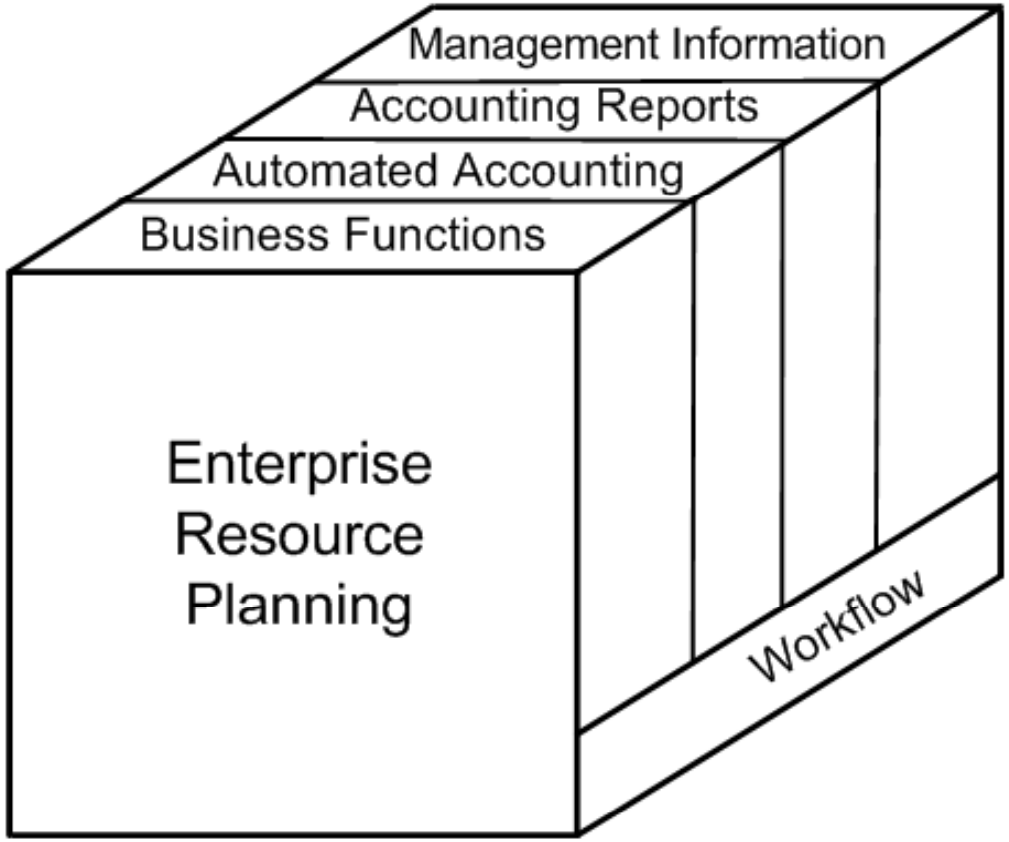
- Traditional Accounting System




Cherry Bekaert LLP
Your guide forward

# *What is an ERP System vs. an Accounting System?*

- ERP System Model




Cherry Bekaert LLP
Your guide forward

# *What are the Characteristics of an ERP System?*

- Multi-layered structure as opposed to a linear structure
- Seamless, integrated functionality
- Automated controls such as three-way match, automated journal entry approval, purchase order management, budgetary controls, etc.
- Automated workflow
  - Result is a change in the way you do business

# *ERP Requirement Types*

- Functional Requirements
  - Business Processes that users can expect to be fully or at least partially automated.
- Technical Requirements
  - Capability of the system to conform to and compliment protocols inherent in the current technology infrastructure.
- Operational Requirements
  - Capability to support the day-to-day functions of business unit users
- Contract Requirements
  - Certain terms and conditions should be addressed here including *limits on the cost of annual maintenance increases*

# *Vendor Selection*

- Experience in your Industry
- Experience with organizations your size
- Experience with your organizations IT infrastructure
- Do they meet all of your Requirements with minimal customization?
- References/Referrals

# *Implementation Type*

- Considerations:
  - Parallel Processing vs. Cut Over
  - Phased vs. Complete
  - Modular vs. Departmental
- Develop a migration plan which includes defined responsibilities and system reconciliation
- Document a detailed audit trail of the implementation process

# *Managing the Implementation*

- Set the Tone at the Top
  - Select Project Sponsor(s)
  - Select a Formal Steering Committee
  - Designate day to day Project Manager(s)
- Define Team Responsibilities and Project Reporting
- Break Up the Project into documented Milestones
- Define acceptance criteria around your Requirements
- Designate Test Team Members
- Define Test Scripts to conduct User Acceptance Testing and track issues
- Train Users and Support Staff

Cherry Bekaert LLP
Your guide forward

# *Post Implementation Process*

- Continue to track problems and issues
- Define a Change Management Process
- Define a New Release Implementation Process
- Plan for on-going training
- Define and plan subsequent enhancements

# *Common Pitfalls*

- Never place total reliance on the Software or Integration Vendor
- Never agree to a technical solution or product that is not fully understood
- Don’t just duplicate the old system
- Try to set Realistic Deadlines
- Document Everything…

# What questions do you have?

Cherry Bekaert LLP
Your guide forward