

The Deloitte logo, consisting of a vertical stack of horizontal bars on the left side of the word "Deloitte".

**Deloitte.**

**ISACA Fall Conference**

**October 4, 2004**

**Introduction to  
General Computer Controls**

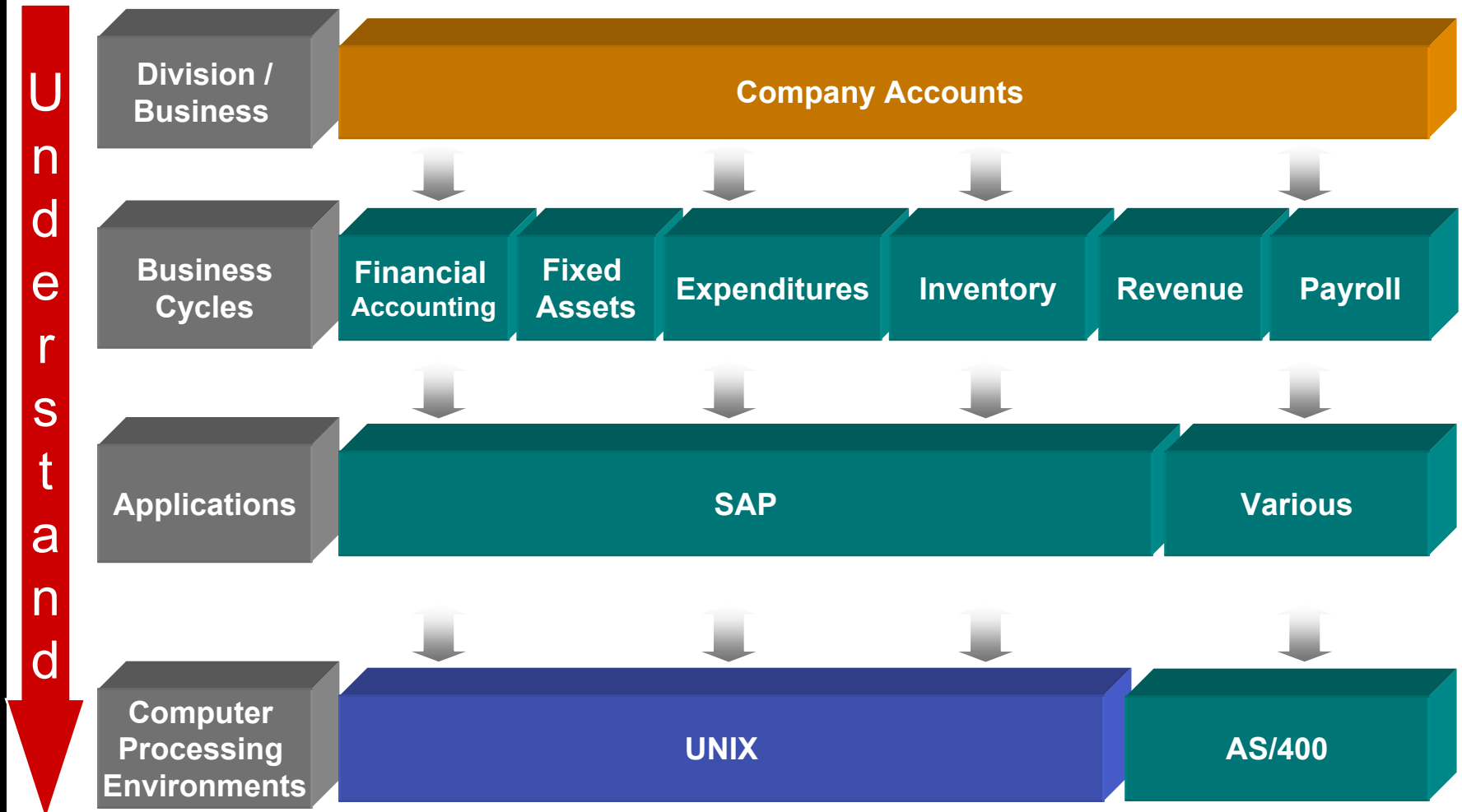
- Ed Byers

- Muna Sheikh

- History of General Computer Controls
- Background Information – Business Cycle Controls, Application Controls, and GCCs
- GCC Control Objectives
- FAQs

# Background information

## Auditing the Company's Key Financial Statement Accounts

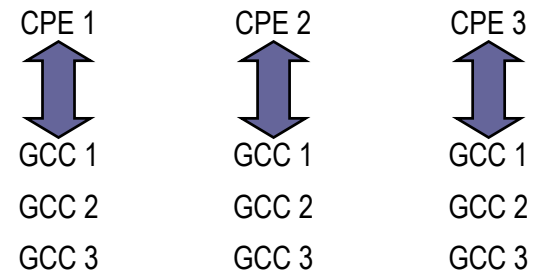


# Background information

- What are General Computer Controls?

Pervasive controls that provide for the integrity of the underlying controls that support the company-wide internal control environment

An application and the corresponding operating system/ platform together constitutes a computer processing environment.



**There may be more than one computer-processing environment within a client and even within one physical location.**

# Background information

How are controls within GCCs and BCCs integrated?

- GCCs are typically pervasive to all financial accounting transactions within a Business Cycle.
- The effectiveness of automated activities (within a given business cycle) depends on the effectiveness of general computer controls.
- For example, Security, a General Computer control area, applies to all of the transactions within a specific business cycle.

## GCCs



- Corporate Network
- Platforms (Unix, AS400, W2K)
- Applications
- Logical and Physical Security
- Change Management

## BCCs



- Application systems supporting business process such as Purchasing, Revenue, Payroll
- Automated controls such as balancing and integrity checks
- Fraud and segregation of duty controls

# IT Framework

Regulatory & Legal  
Policies  
Standards  
Technology trends

## IT Governance

- IT Risk Management
- Oversight
- IT and Business Alignment

## IT Strategy & Planning

- IT Planning
- Strategic Sourcing
- IT organization
- Budget and control

## IT Management

### Program Management

Change Management

Project Management

Quality Assurance

Portfolio Management

### Technology Mgt

- Technology planning
- Architecture design
- Vendor / Product selection

### Operations

- Data Center Ops
- Storage Mgt
- Data Mgt
- Network & Systems Mgt
- Desktop Mgt
- Release Mgt
- Performance Mgt

### Applications

- Development
  - Testing
  - Conversion
  - Implementation
- IT Change Mgt
- Maintenance

### Support

- Vendors / Third Party
- Help desk
- End user support
- Training

### Enterprise Security Architecture and Management

### Disaster Recovery Planning

### IT Human Resources

# General Computer Controls

Understanding the  
Computer Processing  
Environment

Information Security

Operations

Application Systems  
Implementation & Maintenance

Database Implementation &  
Support

Network Support

Systems Software Support

Hardware Support

Business Continuity Planning

Info Resource Strategy & Planning

Relationship with Outsourced  
Vendors

# Information Security

---

Information security is comprised of the following sub-processes:

- Information Security Policies, Procedures, and Organization
  - User Security Administration
  - Application Security
  - Database Security
  - Operating System Security
  - Network Security
  - Physical Security
- 
- Need to assess and prioritize security risks at multiple layers (network, operating system, application and physical layer)
  - Need to understand data classifications, data ownership, and implementation of security policies

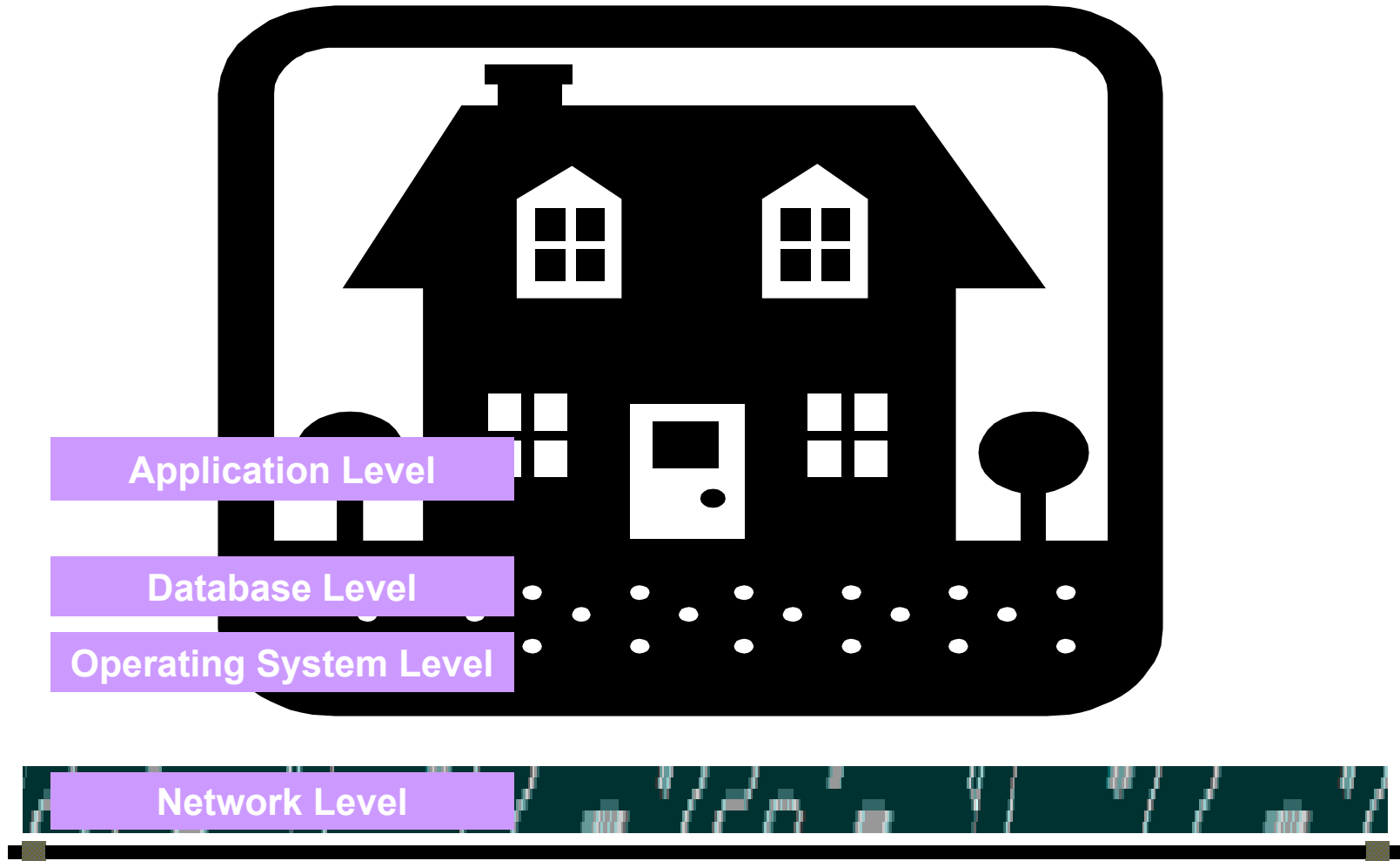
# Information Security

---

## Control Objectives

- Logical security tools and techniques are implemented and configured to enable restriction of access to programs, data, and other information resources.
- Logical security tools and techniques are administered to restrict access to programs, data, and other information resources.
- Physical access restrictions are implemented and administered to ensure that only authorized individuals have the ability to access or use information resources.
- All information resources are subject to appropriate physical and logical security.

# Layered Security Model



Operations is comprised of the following sub-processes:

- Backups and Restores
- Job and Batch Scheduling and Processing
- Monitoring of Applications and supporting Servers
- Value Add areas of Service Level agreements, user training and qualification of Operations personnel

## Control Objectives

- All production programs needed to process batch and on-line transactions and prepare related reports are executed timely and to normal completion.
- Only valid production programs are executed.
- Data is retained in accordance with laws, regulations, and company policy to enable retrieval when needed.
- Various other areas

# Change Management / Change Control

Ensuring that all applications and systems are appropriately:

- Planned
- Approved
- Selected or Designed and Developed
- Tested
- Implemented
- Maintained
- Supported

Application Systems  
Implementation & Maintenance

Database Implementation &  
Support

Systems Software Support

Network Support

These control areas relate to what we might think of as the “**System Development Lifecycle**” (applied to all types of technologies) and processes to support production systems such as **Change Management**, Request Management, Problem Management and Incident Handling.

# Application Systems Implementation & Maintenance

---

## Control Objectives

- New application systems are appropriately implemented and function consistent with management's intentions.
- When new application systems are implemented, existing data that is converted to the new system is complete, accurate, and valid.
- All necessary modifications to existing application systems are implemented timely.
- Modifications to existing application systems are appropriately implemented and the modified application systems function consistent with management's intentions

# Database Implementation & Support

---

## Control Objectives

- The data structure, as defined in the database management system (or its equivalent) is appropriately implemented and functions consistent with management's intentions.
- All necessary modifications to the existing data structure are implemented timely.
- Modifications to the existing data structure are appropriately implemented and the modified data structure functions consistent with management's intentions.

# Systems Software Support

---

## Control Objectives

- New systems software is appropriately implemented and functions consistent with management's intentions.
- All necessary modifications to existing systems software are implemented timely.
- Modifications to existing systems software are appropriately implemented and modified systems software functions consistent with management's intentions.

## Control Objectives

- New network and communication software is appropriately implemented and functions consistent with management's intentions.
- All necessary modifications to existing network and communications software are implemented timely.
- Modifications to existing network and communications software are appropriately implemented and modified network and communications software function consistent with management's intentions.

# General Computer Controls

## GCC – Non Financial Reporting Controls

- **Information Resource Strategy and Planning –**  
Utilizing technology solutions to assist in deploying the company's business level and corporate level strategy.
  - Information systems strategies, plans, and budgets are consistent with the entity's business and strategic goals.
  - The computer processing environments are adequately staffed with appropriately skilled and experienced personnel.
  - Personnel within the computer processing environments receive appropriate training.

# General Computer Controls

---

- **Relationships with Outsourced Vendors** – Policies, procedures, and internal controls to manage relationships with vendors that supply services for an area of General Computer Control.
  - The selection of outsourced vendors is consistent with management's intentions.
  - Outsourced vendors' service levels meet or exceed management's expectations.

# General Computer Controls

---

- **Business Continuity Planning** – Developing an entity-wide plan to maintain and/or restore business operations, in the event of a disaster, at a level and within a time frame that is acceptable to management.
  - In the event of a disaster, essential business processes and information systems can be recovered timely.

# General Computer Controls

---

## Values-Added Areas

- **Hardware Support** – Managing the computing hardware infrastructure. Implementing and maintaining such hardware.
  - New computer hardware is acquired consistent with management's intentions.
  - New computer hardware is appropriately implemented and functions consistent with management's intentions.
  - Computer hardware is maintainable and supportable.
  - Necessary modifications and/or additions to computer hardware are implemented timely.



- What's the right password length?
- In SOX, what are the key GCC areas?
- What's more important – application controls or GCCs?
- Where can I learn more about GCCs?