



# IT Auditing for Non-IT Auditors

Presented by:

Steve Shofner – IT Audit Manager, Williams-Sonoma

Melinda Moy – IT Auditor, Williams-Sonoma



# Learning Objectives

---

- Establish Baseline Understanding of Key Term's & Concepts
- Understand Automated Controls
- Understand The Relationship Between Financial and IT Controls
- Compare IT Auditing to Non-IT Auditing
  - Dispelling Common Myths
- How To Test Common IT General Controls (In A Simple Environment)

# What Is An Audit?

---

- Processes contain risks that the objectives may not be met
- Audits are an evaluation of a process to ensure that certain objectives are met
- Audits focus on controls in the process, which address the risks

# Definitions

---

- What Is A Risk?
  - The hazard or possibility of loss (financial or operational)
- What Is An Objective?
  - The purpose that one's efforts or actions are intended to attain or accomplish (to address risks)
- What Is A Control?
  - A proactive step taken by “management” to accomplish an objective
    - Management is any employee of the firm
    - The term management is used because they are usually responsible for implementing and maintaining effective controls

# Types Of Objectives

---

- Financial Objectives
  - Completeness
  - Accuracy
  - Validity
  - Authorization
  - Real
  - Rights & Obligations
  - Presentation & Disclosure
- IT & Operational Objectives
  - Security
  - Availability
  - Confidentiality
  - Integrity
  - Scalability
  - Reliability
  - Effectiveness
  - Efficiency

**Compliance Audits Could Include Objectives From Both**

# Types of Controls

---

- Automated Controls
  - These are programmed financial controls
  - They are *very* strong
  - The programmed logic will function the same way every time, as long as the logic is not changed
  - Test of one versus a statistical test of many
- Partially-Automated Controls
  - People-enabled controls
  - People rely on information from IT systems (also referred to as Electronic Evidence) for the control to function
- Manual Controls (no IT-Dependence)
  - People enable the control
  - Controls that are 100% independent of IT systems

# Other Ways To Categorize Controls

---

- Prevent Controls
  - The locks on your car doors
- Detect Controls
  - Your car alarm
- Correct Controls
  - Your auto insurance
  - A LoJack system (a device that transmits a signal used by law enforcement to track down your stolen car)

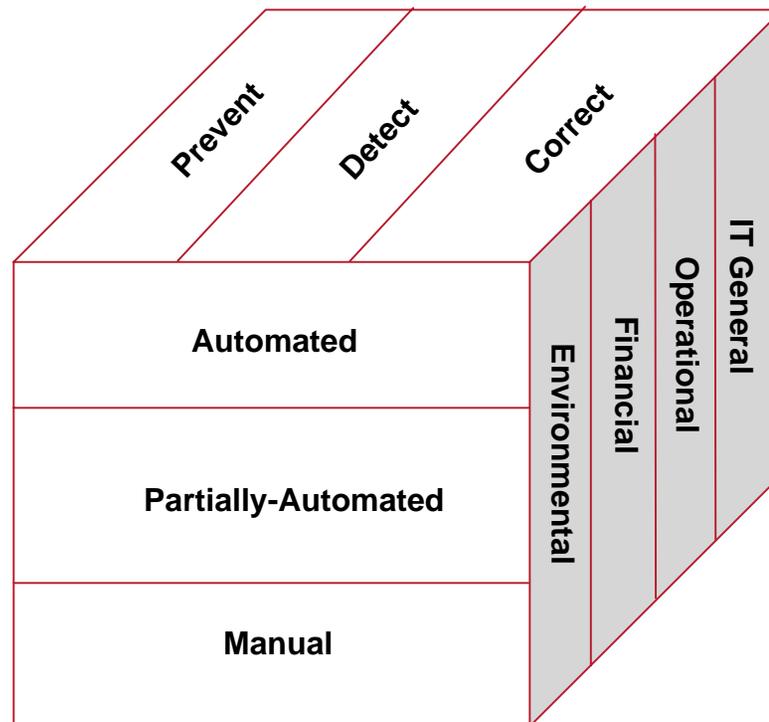
# Yet More Ways To Categorize Controls

---

- Environmental Controls
  - (a.k.a. “Governance”)
- Financial Controls
- Operational Controls
- IT General Controls
  - User Administration
  - Change Management
  - IT Operations
  - Physical Environment

# Controls: Multidimensional

---



# Examples of Controls

---

- Examples:
  - To ensure that only *authorized* payments are made, checks require a signature
  - User access requests must have a supervisor's signature *authorizing* the user's access

*(note the different types of 'transactions')*

# Classifying Controls

---

- To ensure that only *authorized* payments are made, all checks issued require a signature.

- Accomplishes the *financial* objective, *authorized*.
- Someone *manually* signs the check
- An unsigned check *prevents* it from being cashed

- 
- All user requests (on MAC forms) must have a supervisor's signature *authorizing* the user's access.

- Accomplishes the *IT General Control* objective, *authorized*.
- Someone *manually* signs the MAC form
- Unsigned MAC forms will not be processed, thereby *preventing* unauthorized access

# Quiz #1

---

- Classify the controls in the handout



## Mythbusters – Challenge #1

---

- “IT Controls are too technical – I don’t understand what they do”
- Myth, Plausible, or Busted?

# Introduce Case Study

---

Purchase To Pay

A Made-Up

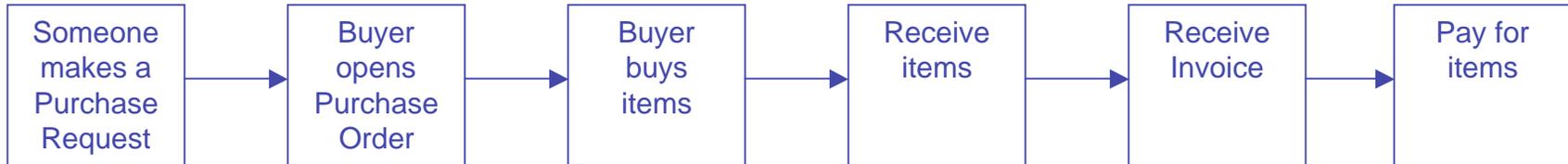
Illustrative

Example Only

- Let's take a look at the mechanics of a process and the related:
  - Objectives
  - Risks
  - Controls

# Purchase To Pay Process

---



- **Financial Objectives**

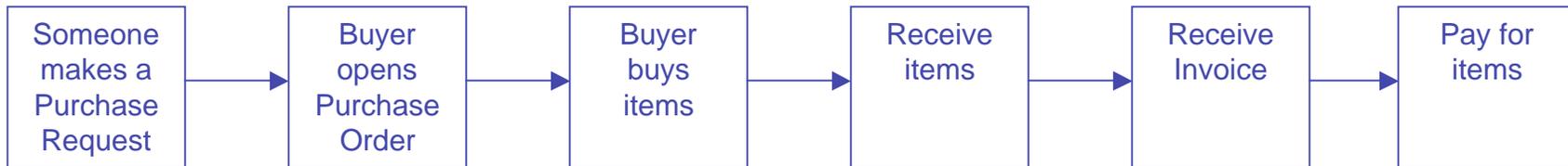
- Completeness
- Accuracy
- Validity
- Authorization
- Real
- Rights & Obligations
- Presentation & Disclosure

- **IT & Operational Objectives**

- Security
- Availability
- Confidentiality
- Integrity
- Scalability
- Reliability
- Effectiveness
- Efficiency

# Purchase To Pay Process

---

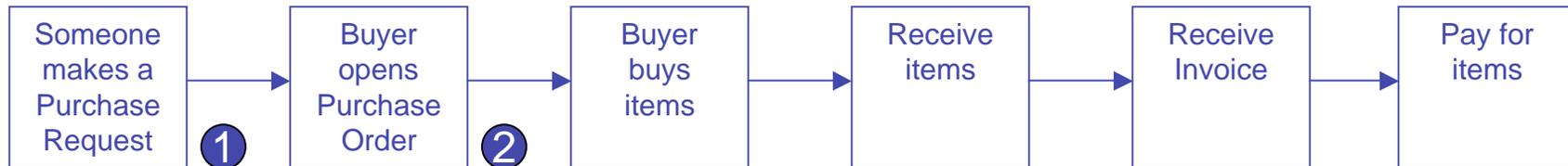


- **Risks:**

- Employee may order too much
- Employee may try to misappropriate goods:
  - Fictitious order to collect check
  - Purchase goods for personal use/gain
- Buyer may not use approved vendor (gaining the benefit of negotiated volume discounts)
- Duplicate or missing items may be received
- Invoice information may not be correct
- Duplicate or missing invoices may be received
- Incorrect payment amount
- Payment sent to wrong address
- Wrong payee on check
- Check may not be signed
- Check may not be cashed by payee

# Purchase To Pay Process

---



- **Risks:**

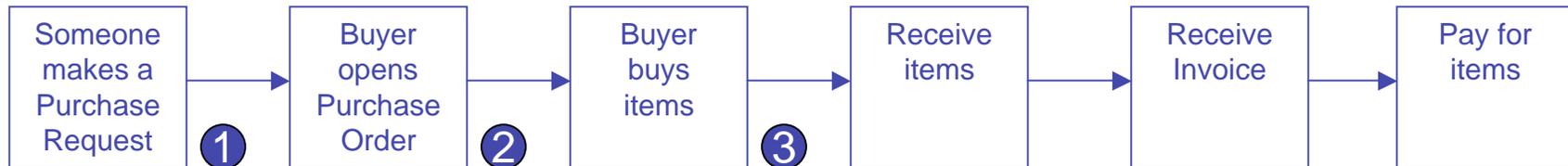
- Employee may order too much or not enough
- Employee may try to misappropriate goods

- **Controls:**

1. All Purchase Requests must be approved by a Manager or above
2. Buyers will only open Purchase Orders upon receipt of an approved Purchase Request

# Purchase To Pay Process

---



- **Risk:**

- Buyer may not use approved vendor (gaining the benefit of negotiated volume discounts)

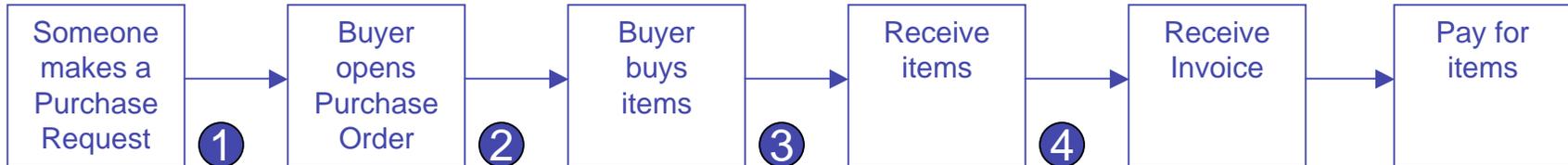
- **3. Control:**

- Goods can only be purchased from vendors who have been pre-approved

*(Assumption: process is in place to approve vendors, and is operating effectively)*

# Purchase To Pay Process

---



- **Risk:**

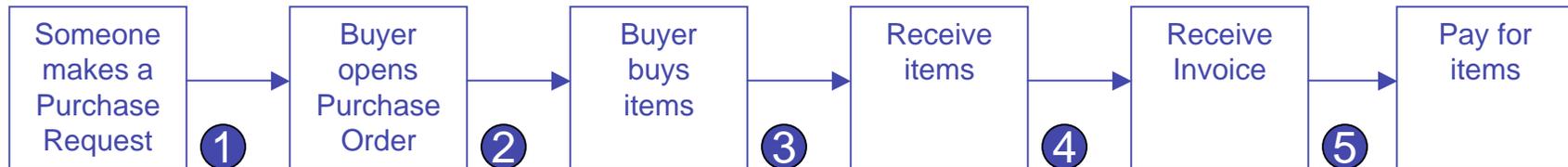
- Duplicate or missing items may be received

- **4. Control:**

- Receiving Clerk counts all items received, ties them to shipping slip, and will only receive complete shipments

# Purchase To Pay Process

---



- **Risks:**

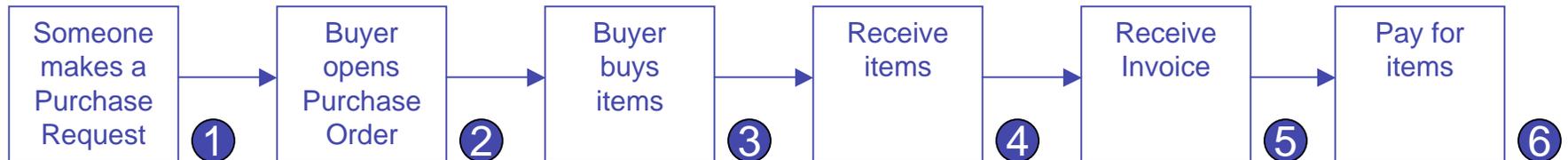
- Invoice information may not be correct
- Duplicate or missing invoices may be received
- Incorrect payment amount

- **Controls:**

5. AP Clerk prepares a voucher package, including:
  - Purchase Order
  - Shipping Slip
  - Invoice
  - Check (Payment)AP Clerk ties out all information across three documents to ensure completeness & accuracy

# Purchase To Pay Process

---



- **Risks:**

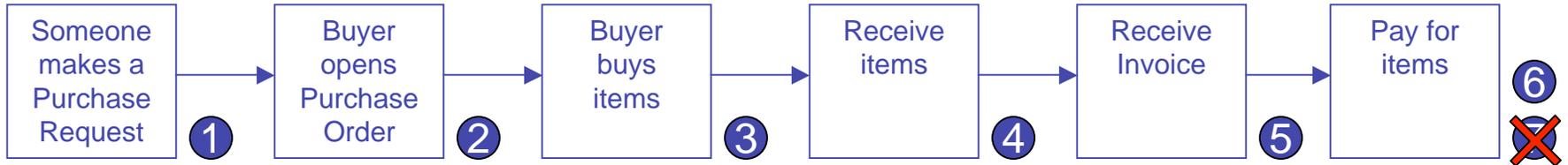
- Payment sent to wrong address
- Wrong payee on check
- Check may not be signed

- **6. Control:**

- VP of Treasury reviews all voucher packages and approves/denies payment (signs checks of approved vouchers)

# Purchase To Pay Process

---



- **Risks:**

- Check may not be cashed by payee

## 7. Control:

- ???

# Comparison

Objective	Manual Control	Automated Control
All Purchase Requests must be approved by a Manager or above	Manager signs purchase request form (hardcopy)	Manager clicks approval in application
Buyers will only open Purchase Orders upon receipt of an approved Purchase Request	Buyer compares signature to list of approvers	Application compares user to list of approvers
Goods can only be purchased from vendors who have been pre-approved	Buyer only purchases from list of approved vendors	PO system provides options in a drop-down menu, populated from a list of approved vendors.
Receiving Clerk counts all items received, ties them to shipping slip, and will only receive complete shipments	Receiving Clerk manually performs control	<none>

# Comparison

Objective	Manual Control	Automated Control
<p>AP Clerk prepares a voucher package, including:</p> <ul style="list-style-type: none"><li>• Purchase Order</li><li>• Shipping Slip</li><li>• Invoice</li><li>• Check (Payment)</li></ul> <p>AP Clerk ties out all information across three documents to ensure completeness &amp; accuracy</p>	<p>AP Clerk ties out all information across three sources</p>	<p>Application ties out all information across all three sources, and... (see next control)</p>
<p>VP of Treasury reviews all voucher packages and approves/denies payment (signs checks of approved vouchers)</p>	<p>VP of Treasury signs checks</p>	<p>Application automatically prints checks for all matching information, using signature block</p>



## Mythbusters – Challenge #1

---

“IT Controls are too technical – I don’t understand what they do”

Automated controls don’t do anything that people weren’t already doing.

**Myth Busted!**

# Automated Controls – We LOVE them!

---

- Automated Controls
  - These are programmed financial controls
  - They are *very* strong
  - The programmed logic will function the same way every time, as long as the logic is not changed
  - They are easier to test: a test of one versus a statistical test of many



## Mythbusters – Challenge #2

---

- “Automated Controls are too technical – I don’t understand all the technical stuff required to test them”
- Myth, Plausible, or Busted?

# Automated Controls: Test Strategy

---

1. Determine the programmed logic
  - Usually a configuration setting
  - Sometimes setting is “unconfigurable” (programmed into the application, and cannot be changed without changing program code)
2. Follow one example of each *type* of transaction
  - This confirms that there isn’t anything ‘upstream’ or ‘downstream’ that may affect the outcome

# Automated Controls: Test Strategy

---

## Example:

1. All Purchase Requests must be approved by a Manager or above

1. Get a screen-shot of the configuration setup screen showing this control is configured:

Purchase Request Configurations : Form

Purchase Requests Must Be Approved:

Location of Authorized Approver File: C:/Program Files/Purchase Requestor/Authv

Second-Level Approval:

Location of Second-Level Authorized Approver File: a:/Program Files/Purchase Requestor/Secor

Record: 1 of 1

# Automated Controls: Test Strategy

## Example:

1. All Purchase Requests must be approved by a Manager or above

Purchase Request : Form

Purchase Request Number: AB5849635

Item Descripti	Item #	Quantity	Price
Pencils	5698	25	\$2.99
Paper	8869	2	\$27.99

Approver: John Doe

Record: 1 of 1

1. Get a screen-shot of the configuration setup screen showing this control is configured.
2. Observe one completed purchase request and validate that the approver was on the authorized approver list.

Purchase Request System  
Report #: PR12213  
Authorized Approvers

Report Run Date:  
August 15, 2007

Name	Title
George Washington	Chief Executive Officer
John Keynes	Chief Financial Officer
Benjamin Franklin	Chief Operating Officer
Thomas Jefferson	Chief Administrative Officer
Paul Revere	SVP Public Relations
John Doe	Office Manager
Samuel Adams	Floor Manager
John Adams	VP Internal Audit

# Automated Controls: Test Strategy

---

## Example:

1. All Purchase Requests must be approved by a Manager or above

1. Get a screen-shot of the configuration setup screen showing this control is configured.
2. Observe one completed purchase request and validate that the approver was on the authorized approver list.
3. You're done!



## Mythbusters – Challenge #2

---

“Automated Controls are too technical – I don’t understand all the technical staff required to test them”

You can test these controls, with a little help from your friends (IT Administrators)

**Myth Busted!**

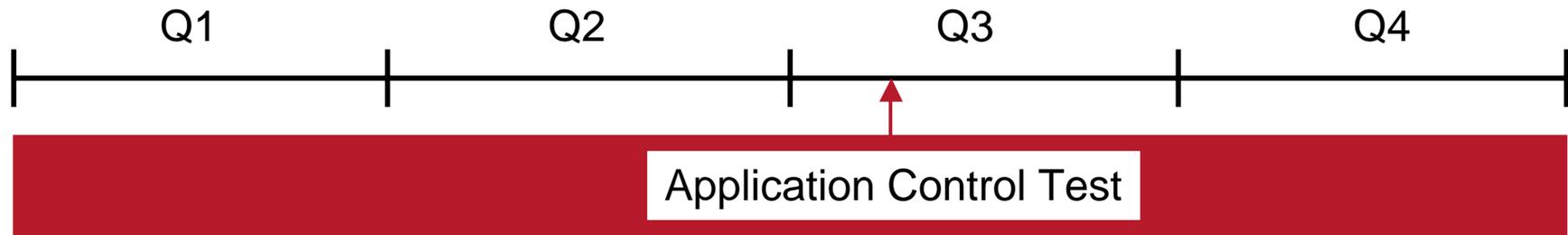
# Automated Controls – We LOVE them!

---

- Automated Controls
  - These are programmed financial controls
  - They are *very* strong
  - The programmed logic will function the same way every time, as long as the logic is not changed
  - They are easier to test: a test of one versus a statistical test of many

# Expanding Coverage Beyond ‘A Point In Time’

---



## IT General Controls

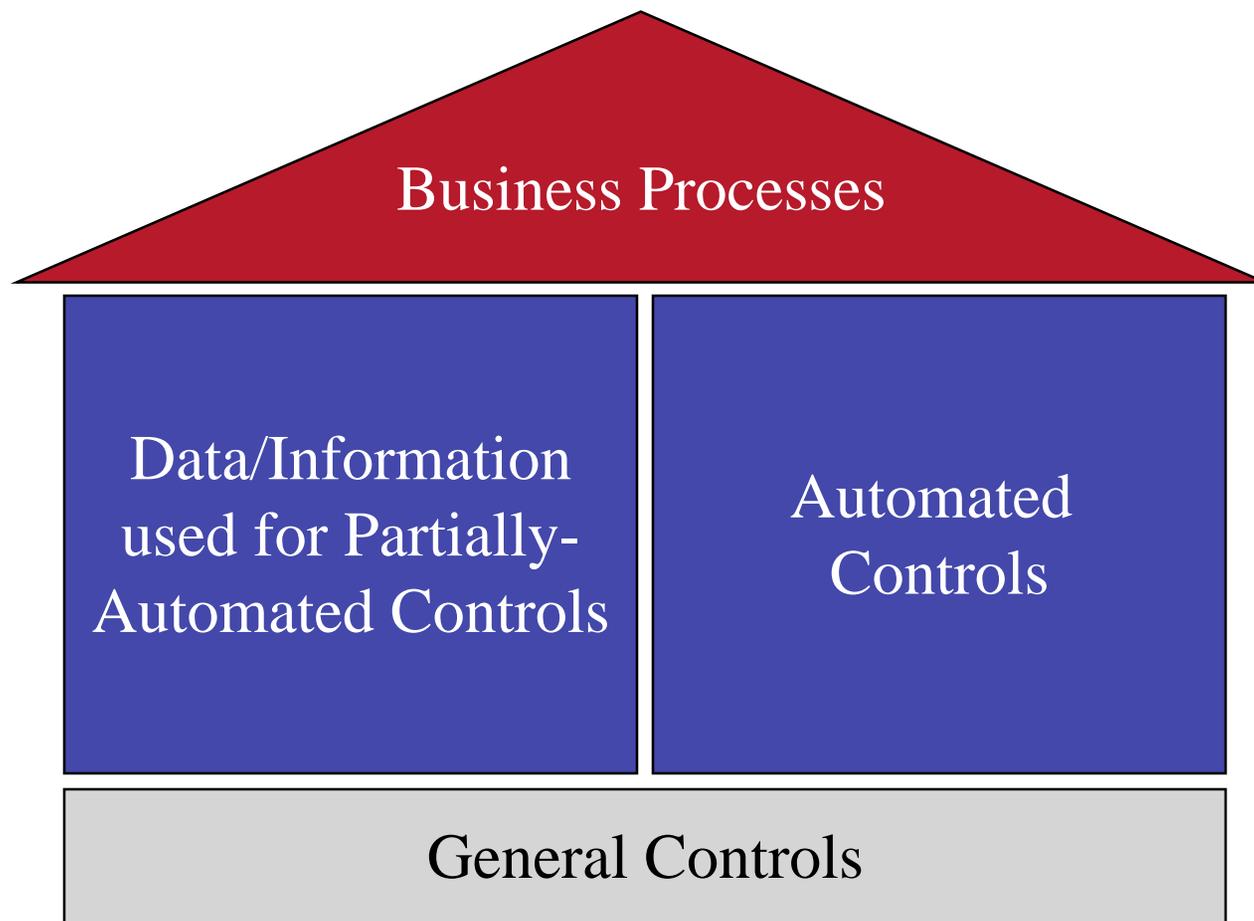
# IT General Controls

---

- ★ Change Management
- ★ User Administration
  - IT Operations
  - Physical Environment

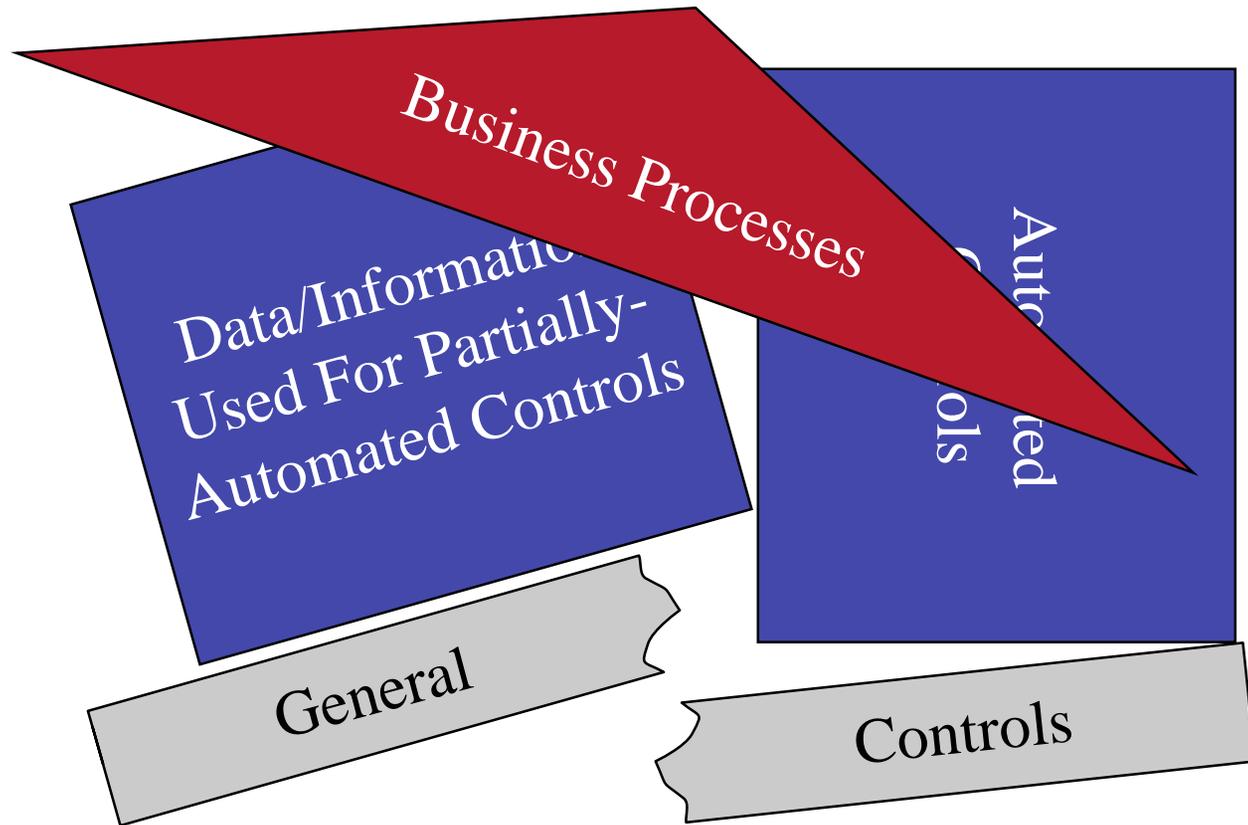
# Effective General Controls

---



# Without Effective General Controls

Potential For Significant Problems Exists





## Mythbusters – Challenge #3

---

- “IT General Controls is all technical stuff...completely out of my realm– I don’t understand all the technical stuff required to test them”
- Myth, Plausible, or Busted?

# IT Change Management

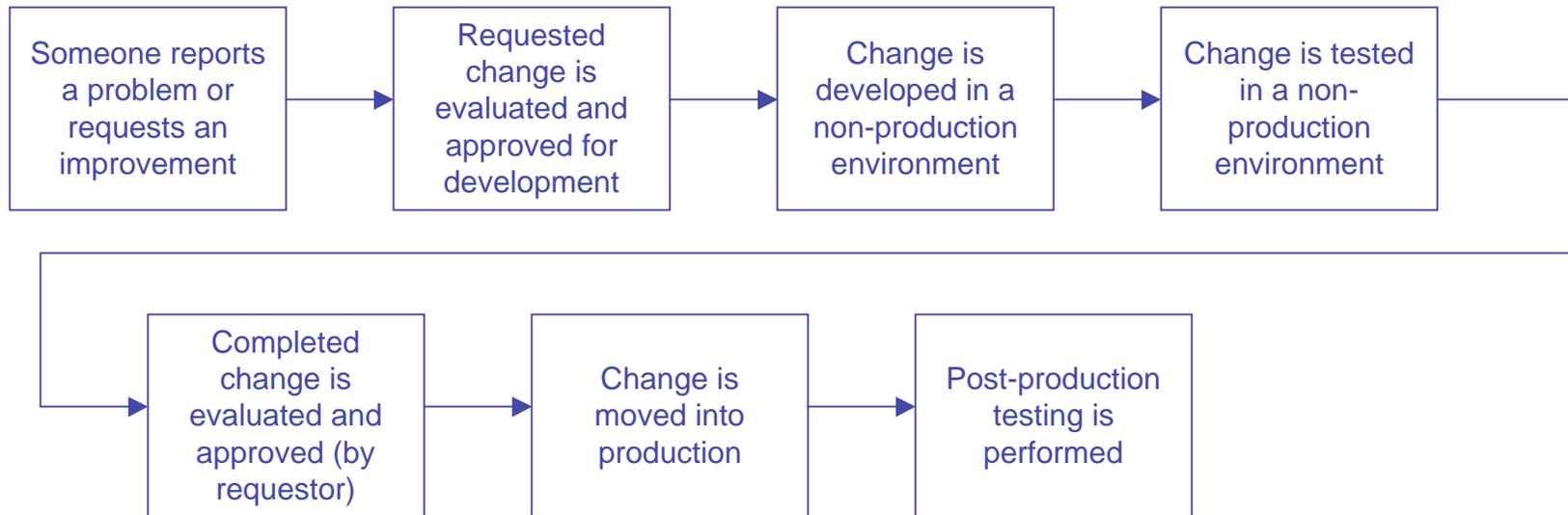
---

- Processes to manage changes to:
  - Program code
  - Configurations
- Objective:
  - Ensure that automated controls aren't inappropriately altered
  - Ensure that data integrity isn't inappropriately affected

**Note:** Fraud is not the primary concern; It's ensuring that good people aren't making honest mistakes.

# Typical Change Management Process

---



**It's a people-driven process**

# Testing Typical Change Management Controls

---

- Get a system generated list of changes
- Select a sample (usually 20-50 changes or 10-20%, whichever is smaller)
- Obtain and review change request forms for evidence of key controls

# User Administration

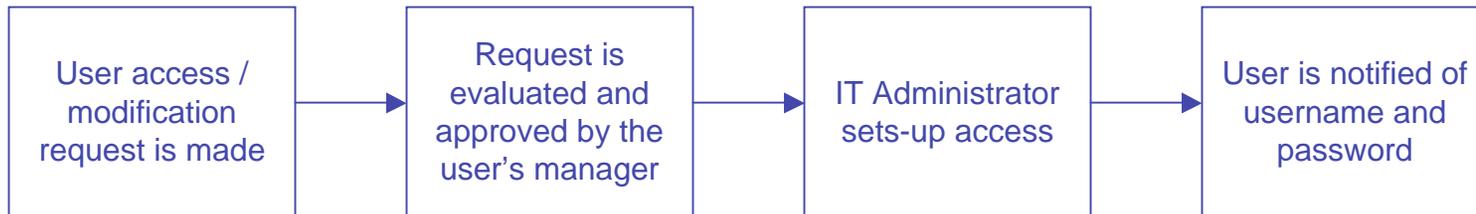
---

- Processes to:
    - Add user access
    - Modify user access
    - Remove user access
- } These two are usually the same process
- Objective:
    - Preventing (or timely detecting of) unauthorized access

# Typical User Administration Process

---

## New / Modifications:



## Removing:



**They are people-driven processes**

# Testing Typical User Administration Controls

---

## New Users / Modifications

- Get a list of change requests
- Select a sample (usually 20-50 changes or 10-20%, whichever is smaller)
- Request change forms and review for key controls

## Removals

- Get a list of terminated employees
- Select a sample (usually 20-50 changes or 10-20%, whichever is smaller)
- Look on system and determine if the user accounts are disabled or removed

# Leading Practice

---

- User Access Reviews: Regularly re-validating all users' access levels on all systems
- This helps prevent:
  - Excessive levels of access
  - Terminated users
  - Potential process problems
- It's a good catch-all detect control



## Mythbusters – Challenge #3

---

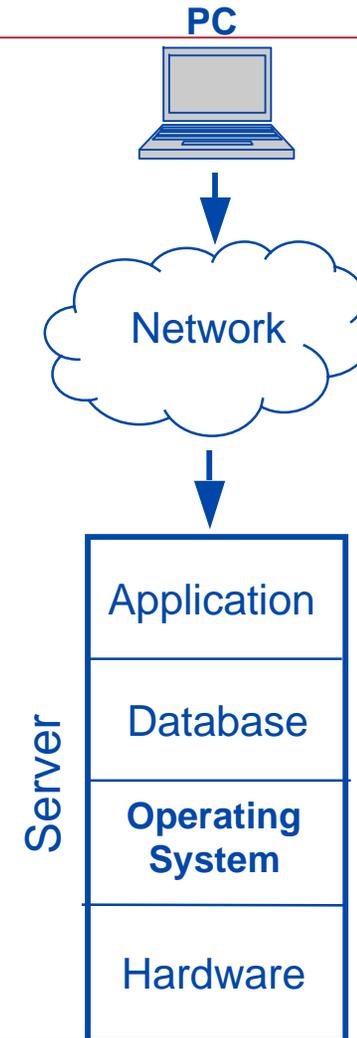
“IT General Controls is all technical stuff, completely out of my realm– I don’t understand all the technical stuff required to test them”

These processes are people-driven and non-technical. You *can* test them.

# When To Bring In “The Experts”

---

- There are many layers of technology that users pass on the “access path” to financial applications and data.
- There are different risks at each level. These risks need to be evaluated at each level.
- Our scope, depth, and approach are different for each.



# When To Bring In “The Experts:” IT Operations

---

- Main Focus Is On Availability of Systems:
  - Job Scheduling
  - Monitoring
  - Problem/Incident Management
  - Business Continuity Planning (BCP) / Disaster Recovery Planning (DRP)
    - Including Backups & Recovery
  - Antivirus / Anti-Spyware / etc.

# When To Bring In “The Experts:” Physical Environment

---

- Also Focused On Availability Of Systems:
  - Access Controls (usually Card Keys)
  - Air Conditioning
  - Leak Detection
  - Fire Suppression
  - Power Conditioning
  - Uninterrupted Power Supplies (or “UPS,” a Battery Backup)
  - Backup Generators

# Any Unanswered Questions?

---

