ISACA®
Serving IT Governance Professionals
San Francisco Chapter

IT Auditing for Non-IT Auditors

Part 1 (Session C11)

Presented by:
Steve Shofner, CISA
Stephen.R.Shofner@kp.org

Learning Objectives

- Part 1 (Session C11)
  - 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

Learning Objectives

- Part 2 (Session C12)
  - How To Test Common IT General Controls (In A Simple Environment)
    - User Access
    - Change Management
    - Computer Operations
    - Physical Environment
    - Determining When To Call ‘The Experts’

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

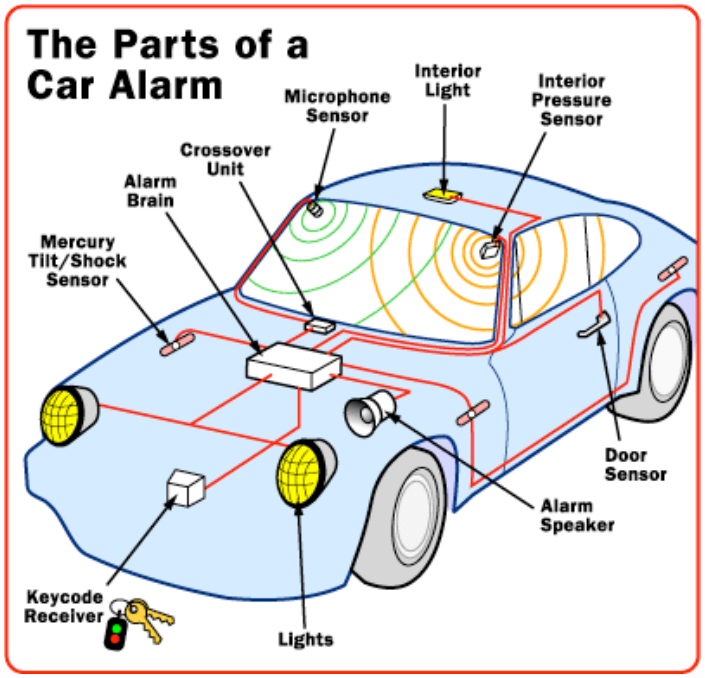
Compliance Audits Could Include Objectives From Both

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

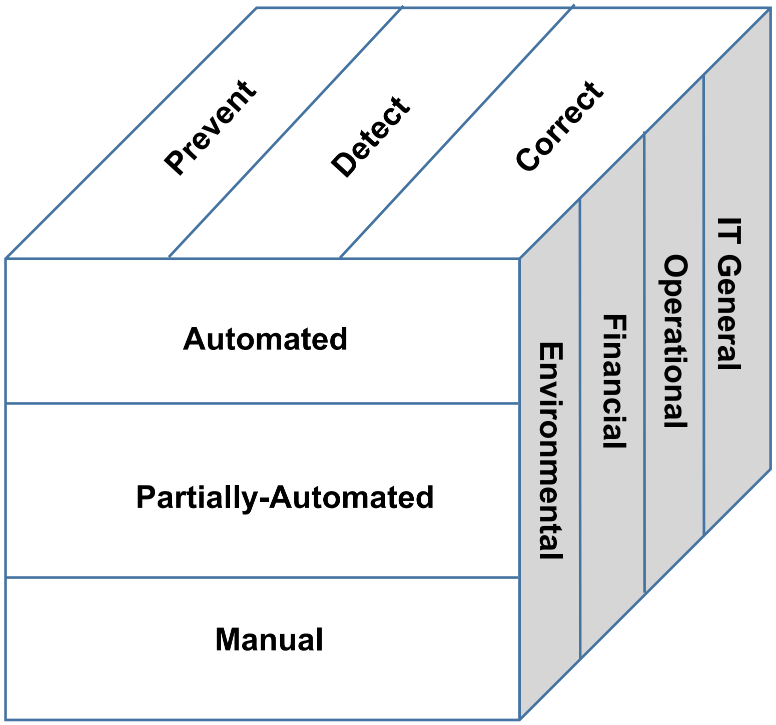
- Prevent Controls
  - The locks on your car doors
- Detect Controls
  - Your car alarm
- Correct Controls
  - Your auto insurance
  - A LoJack system (a device that transmits a signal used by law enforcement to track down your stolen car)



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?

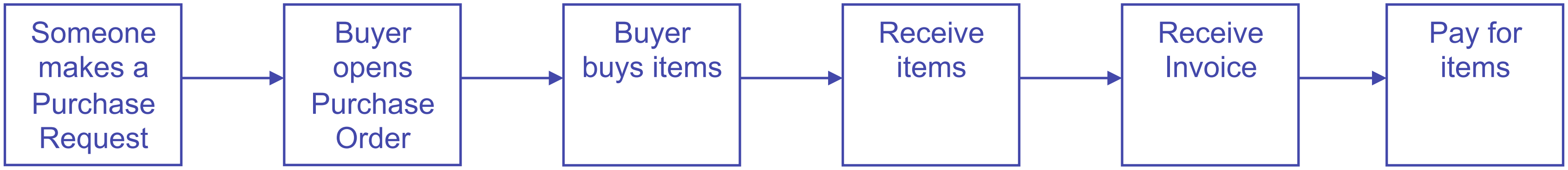
Introduce Case Study

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

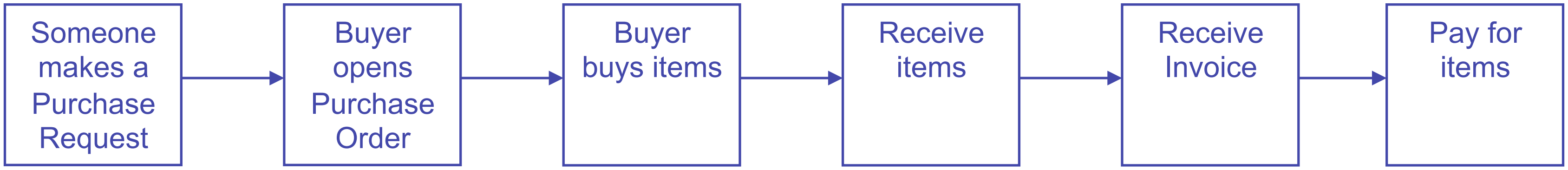


- Financial Objectives
  - Completeness
  - Accuracy
  - Validity
  - Authorization
  - Real
  - Rights & Obligations
  - Presentation & Disclosure

- IT & Operational Objectives
  - Security
  - Availability
  - Confidentiality
  - Integrity
  - Scalability
  - Reliability
  - Effectiveness
  - Efficiency

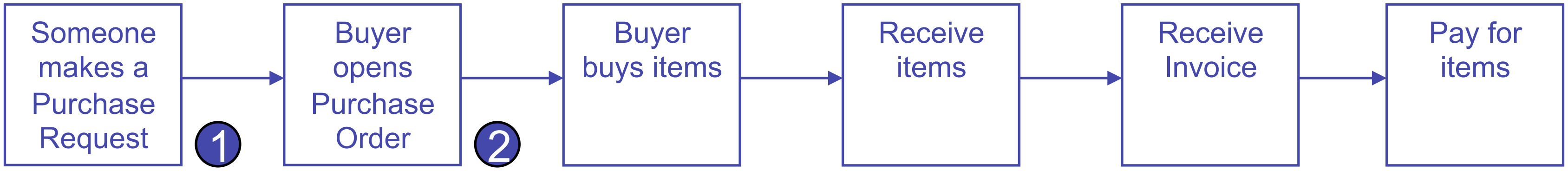
ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Purchase To Pay Process


Someone makes a Purchase Request → Buyer opens Purchase Order → Buyer buys items → Receive items → Receive Invoice → Pay for items

- **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



Someone makes a Purchase Request

1

Buyer opens Purchase Order

2

Buyer buys items

Receive items

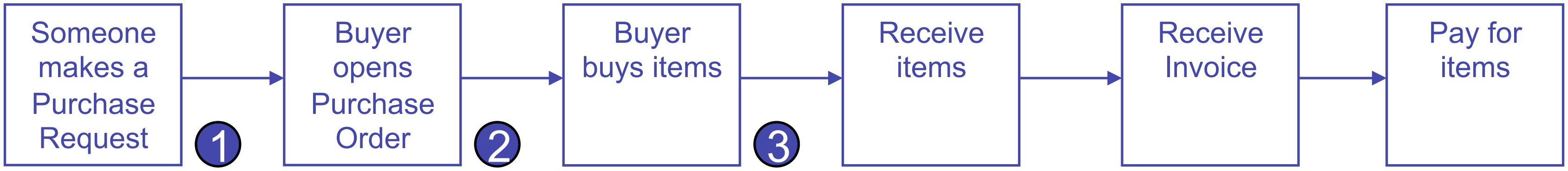
Receive Invoice

Pay for items

- **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



Someone makes a Purchase Request

1

Buyer opens Purchase Order

2

Buyer buys items

3

Receive items

Receive Invoice

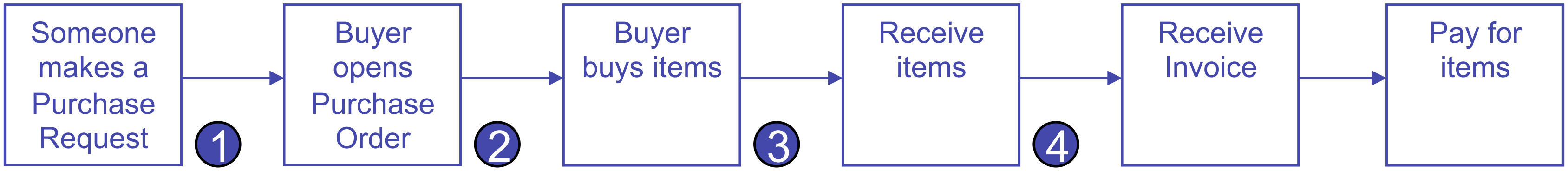
Pay for items

- **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

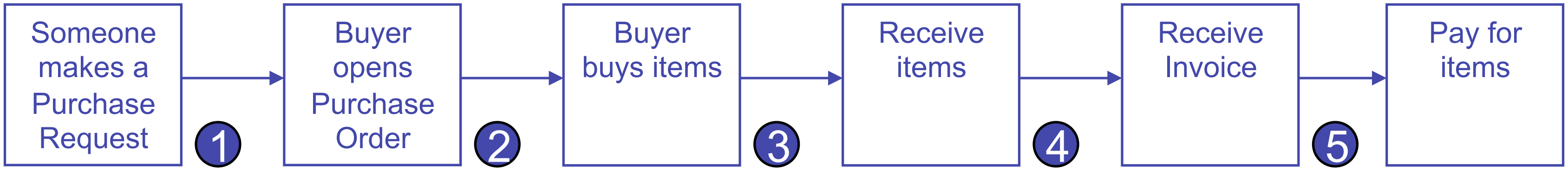


- **Risk:**
  - Duplicate or missing items may be received

4. **Control:**
   - Receiving Clerk counts all items received, ties them to shipping slip, and will only receive complete shipments

ISACA® Serving IT Governance Professionals
San Francisco Chapter

Purchase To Pay Process



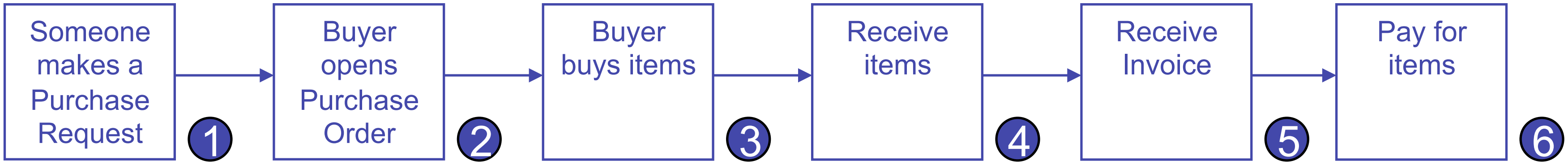
- **Risks:**
  - Invoice information may not be correct
  - Duplicate or missing invoices may be received
  - Incorrect payment amount

- **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

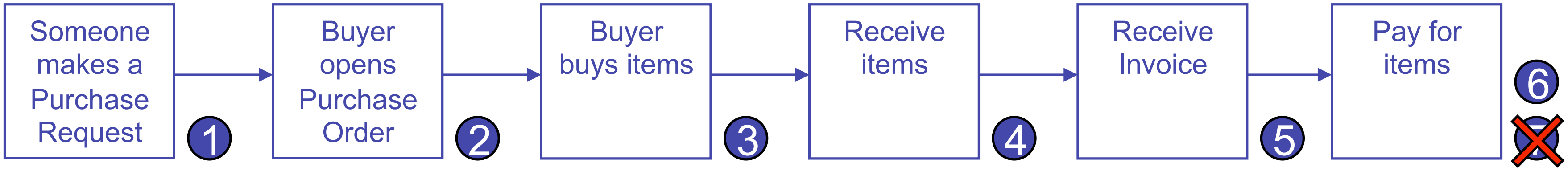


- **Risks:**
  - Payment sent to wrong address
  - Wrong payee on check
  - Check may not be signed

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
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	AP Clerk ties out all information across three sources	Application ties out all information across all three sources, and… (see next control)
VP of Treasury reviews all voucher packages and approves/denies payment (signs checks of approved vouchers)	VP of Treasury signs checks	Application automatically prints checks for all matching information, using signature block

Mythbusters Challenge #1

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

Myth Busted!

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

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

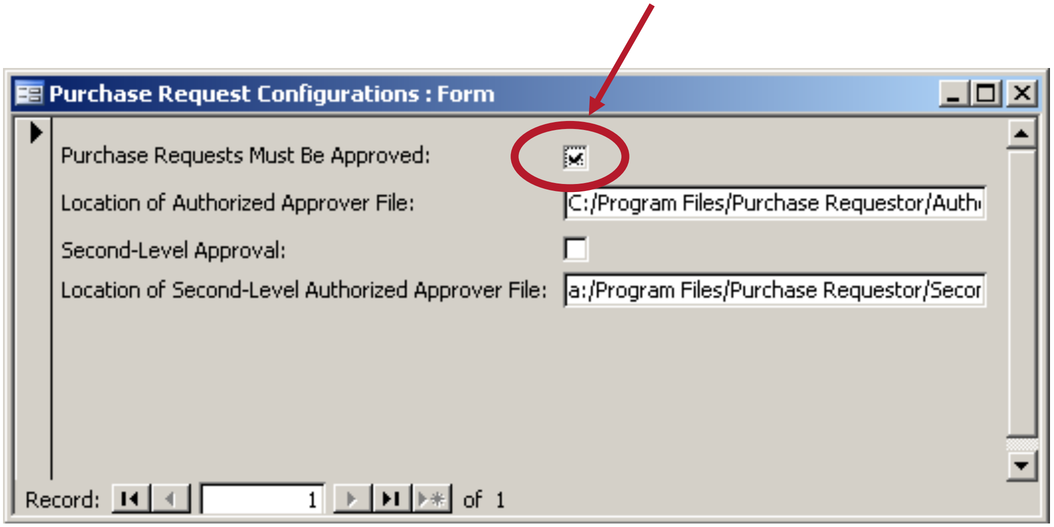
1. Determine the programmed logic
   - Usually a configuration setting
   - Sometimes setting is “unconfigurable” (programmed into the application, and cannot be changed without changing program code)
2. Follow one example of each *type* of transaction
   - This confirms that there isn’t anything ‘upstream’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

Second-Level Approval: □

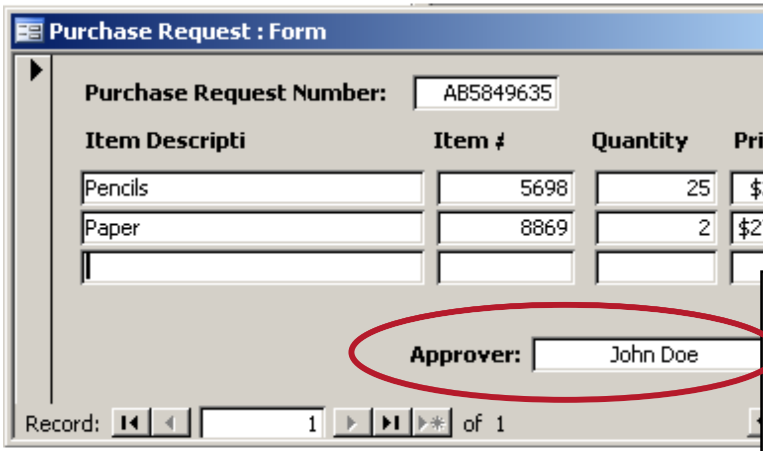
Location of Second-Level Authorized Approver File: a:/Program Files/Purchase Requestor/Secor

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

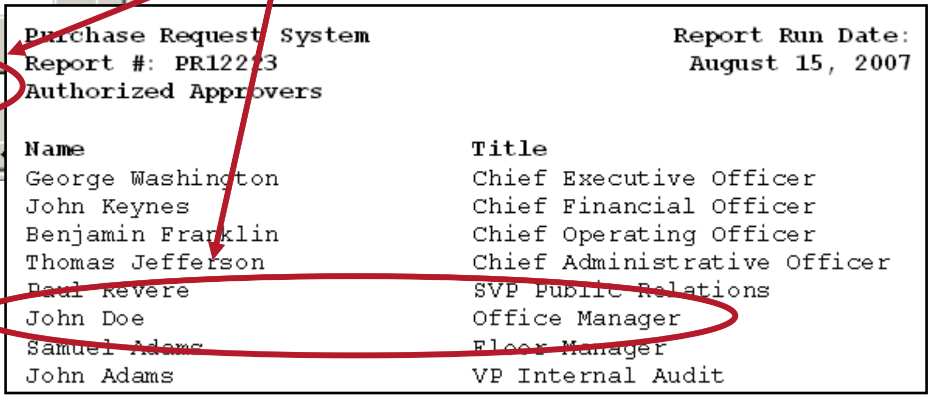
Item Descripti	Item #	Quantity	Price
Pencils	5698	25	$2.99
Paper	8869	2	$27.99

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 Run Date:
Report #:  PR12223                                  August 15, 2007
Authorized Approvers

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 stuff required to test them.”

<u>You</u> *can* test these controls, with a little help from your friends (IT Administrators)

Myth Busted!

Checkpoint

- Covered so far:
  - 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

- Coming up (next session)
  - How To Test Common IT General Controls (In A Simple Environment)

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

IT Auditing for Non -IT Auditors

Part 2 (Session C12)

Learning Objectives

- Part 1 (Session C11)
  - 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

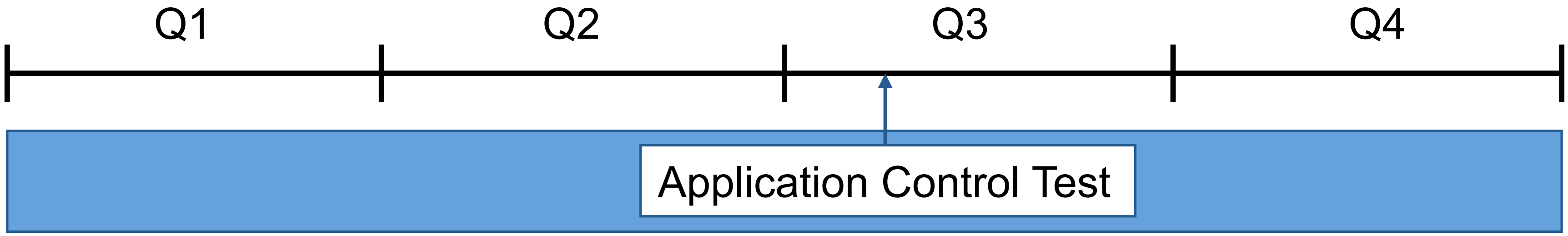
Learning Objectives

- Part 2 (Session C12)
  - How To Test Common IT General Controls (In A Simple Environment)
    - User Access
    - Change Management
    - Computer Operations
    - Physical Environment
    - Determining When To Call ‘The Experts’

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”

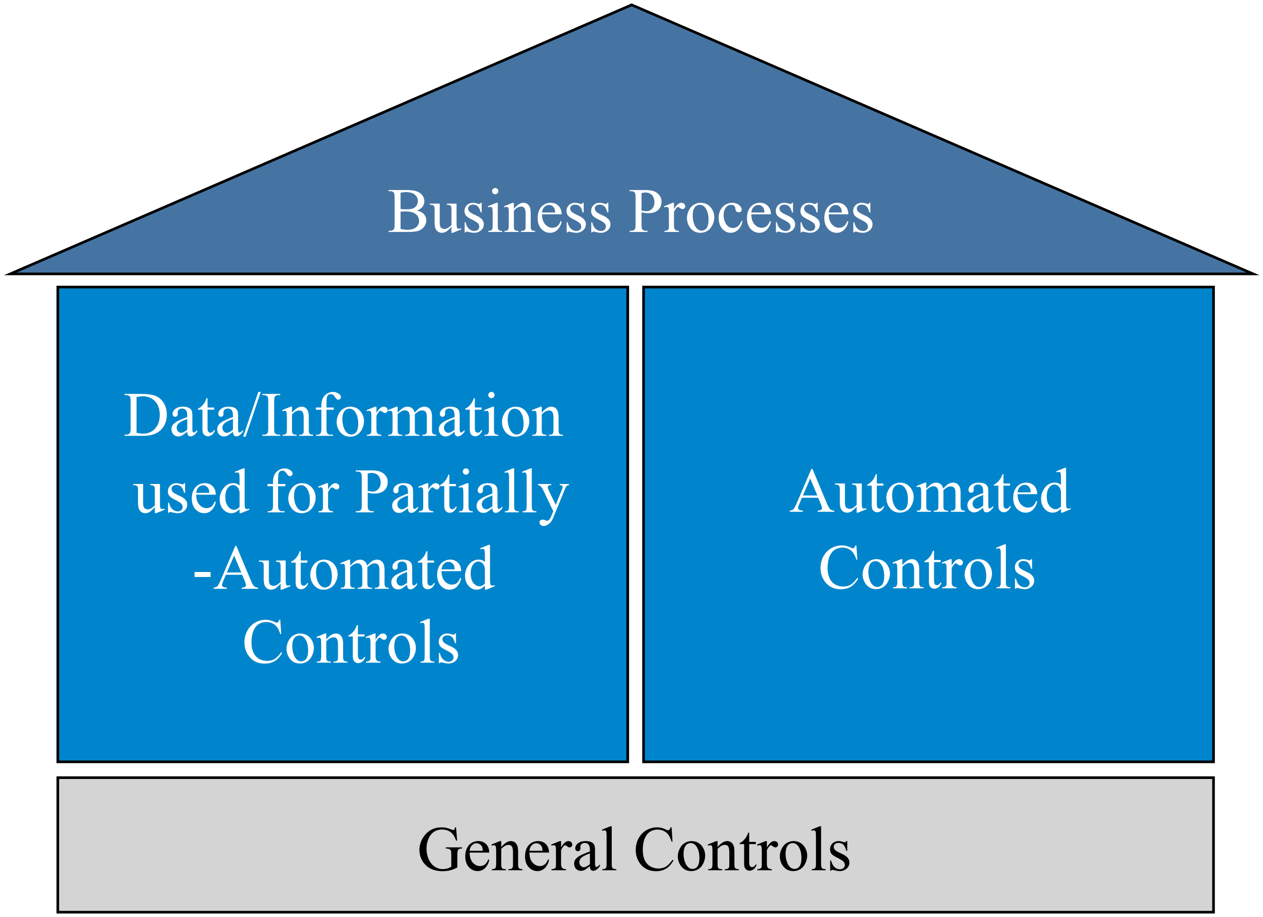


IT General Controls

IT General Controls

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

Effective General Controls



Business Processes

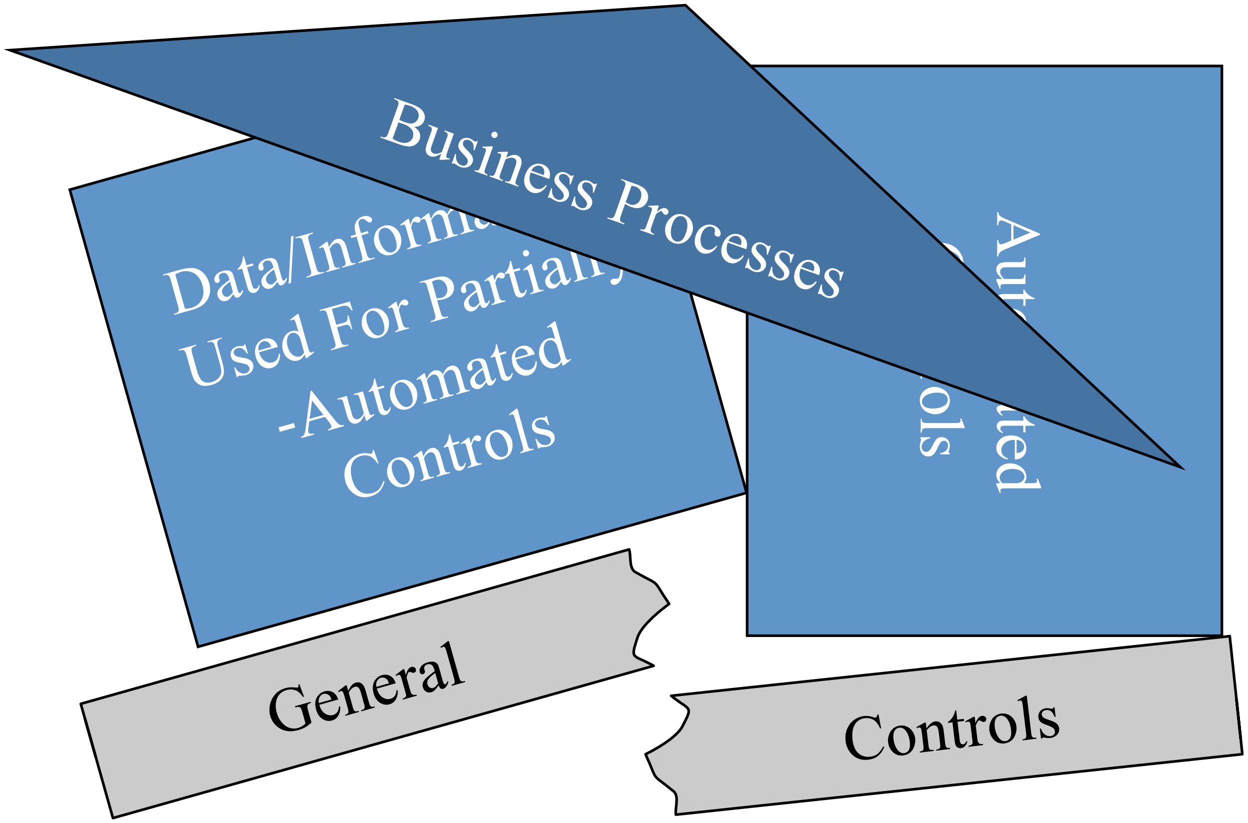
Data/Information used for Partially -Automated Controls

Automated Controls

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?

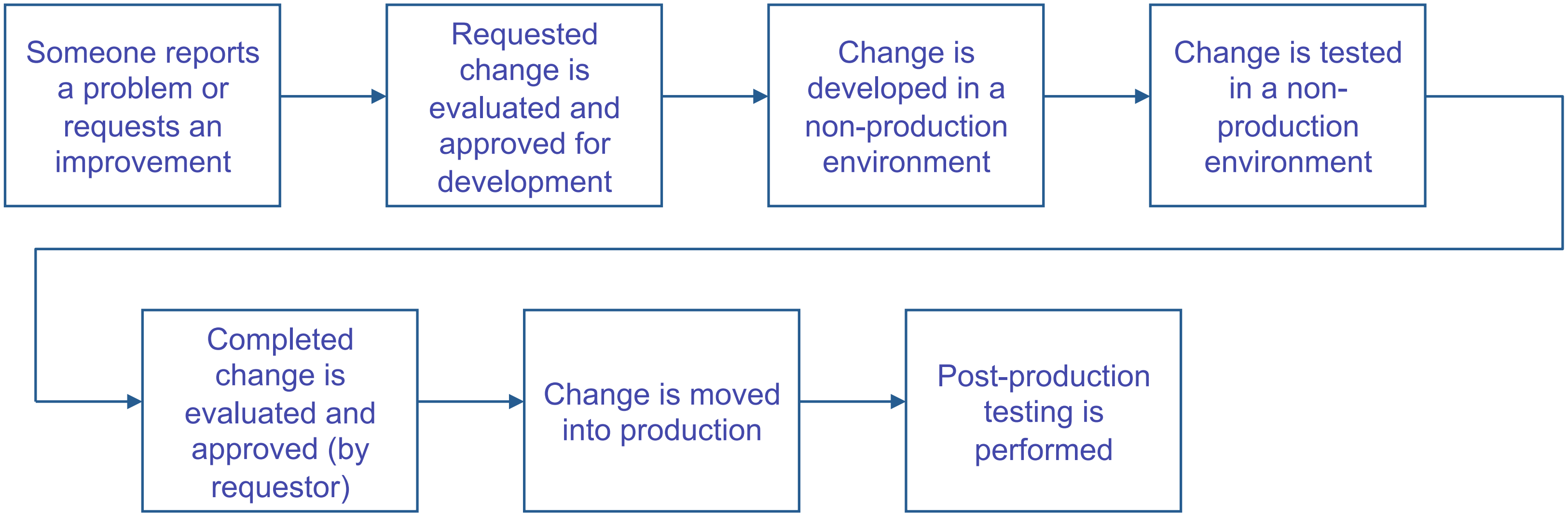
IT Change Management

- Processes to manage changes to:
  - Program code
  - Configurations

- Objective:
  - Ensure that <u>automated controls aren't inappropriately altered</u>
  - Ensure that <u>data integrity isn't inappropriately affected</u>

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

Typical Change Management Process


Someone reports a problem or requests an improvement
Requested change is evaluated and approved for development
Change is developed in a non-production environment
Change is tested in a non-production environment
Completed change is evaluated and approved (by requestor)
Change is moved into production
Post-production testing is performed

It's a <u>people-driven</u> process

Testing The Process

- Four Basic Steps (for most cases in a ‘simple environment’)
  - Process Narrative
  - Walkthrough
  - Testing Documentation
  - Reporting

Process Narrative

- Narratives - Documents Your Understanding Of The Process And Related Controls
  - Different that policy, procedure, & standard documents (although, those documents can be leveraged)
  - At a minimum, Narratives should include:
    - Background
    - Description of Controls
    - Information Necessary For Testing Controls (Who, What, Where, Why, When, How)
  - *For testing purposes*, that is *all* you want

Walkthroughs & Testing Docs

- Walkthroughs – A "Test of One"
  - Confirms Your Understanding Of Controls
  - Allows you to identify any problems in pulling populations or samples
- Testing Documentation
  - Four Basic Sections
    - Objective
    - Procedures
    - Results
    - Conclusion

The Reperformance Standard

- When documenting your work, you should ensure that a reasonably-skilled auditor would be able to review your workpapers (and related evidence) and:
  - Understand what you did any why, and
  - See the same evidence that you saw
  - They should be able to ‘reperform’ your work and reach the same conclusion you did, *based on the information presented in your workpapers and supporting evidence only*.
- They should not need to:
  - Ask clarifying questions
  - Request and review information that is not included in the testing documentation

Reporting

- Reporting communicates the results of testing
- Typically has three sections:
  - Results: The facts, and just the facts
  - Implications / Business Risk: Why should the company care?
  - Recommendation: What should the company do about it?

Testing Typical Change Management Controls

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

Evidence

- Four types:
  - Inquiry
  - Observation
  - Examination
  - Reperformance

User Administration

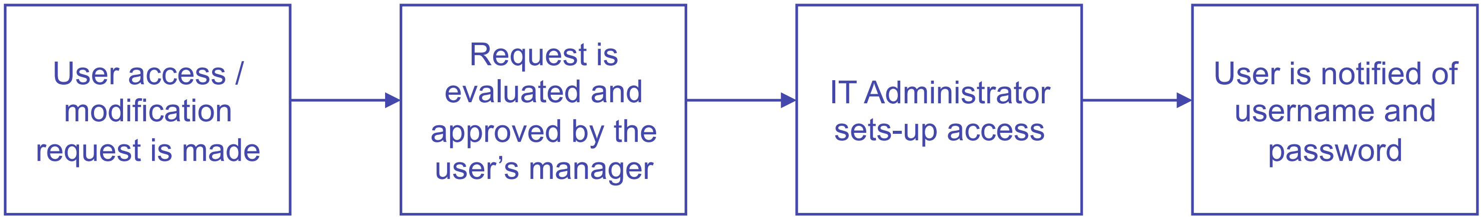
- Processes to:
  - Add user access
  - Modify user access
  - Remove user access

These two are usually the same process

- Objective:
  - Preventing (or timely detecting of) unauthorized access

Typical User Administration Process

New / Modifications:



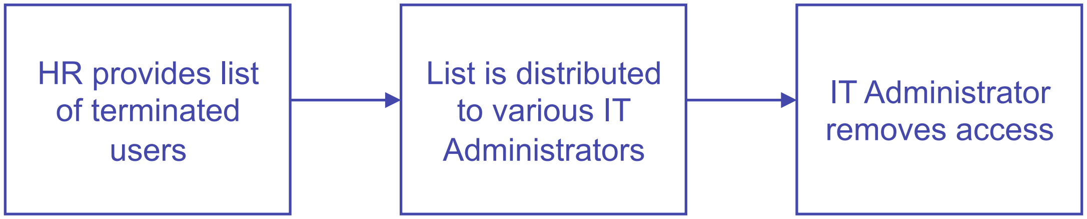
User access / modification request is made

Request is evaluated and approved by the user's manager

IT Administrator sets-up access

User is notified of username and password

Removing:



HR provides list of terminated users

List is distributed to various IT Administrators

IT Administrator removes access

They are <u>people-driven</u> processes

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Testing Typical User Administration Controls

New Users / Modifications

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

Removals

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

Exercise #1

- Complete the testing document
- Conclude on the results

Leading Practice

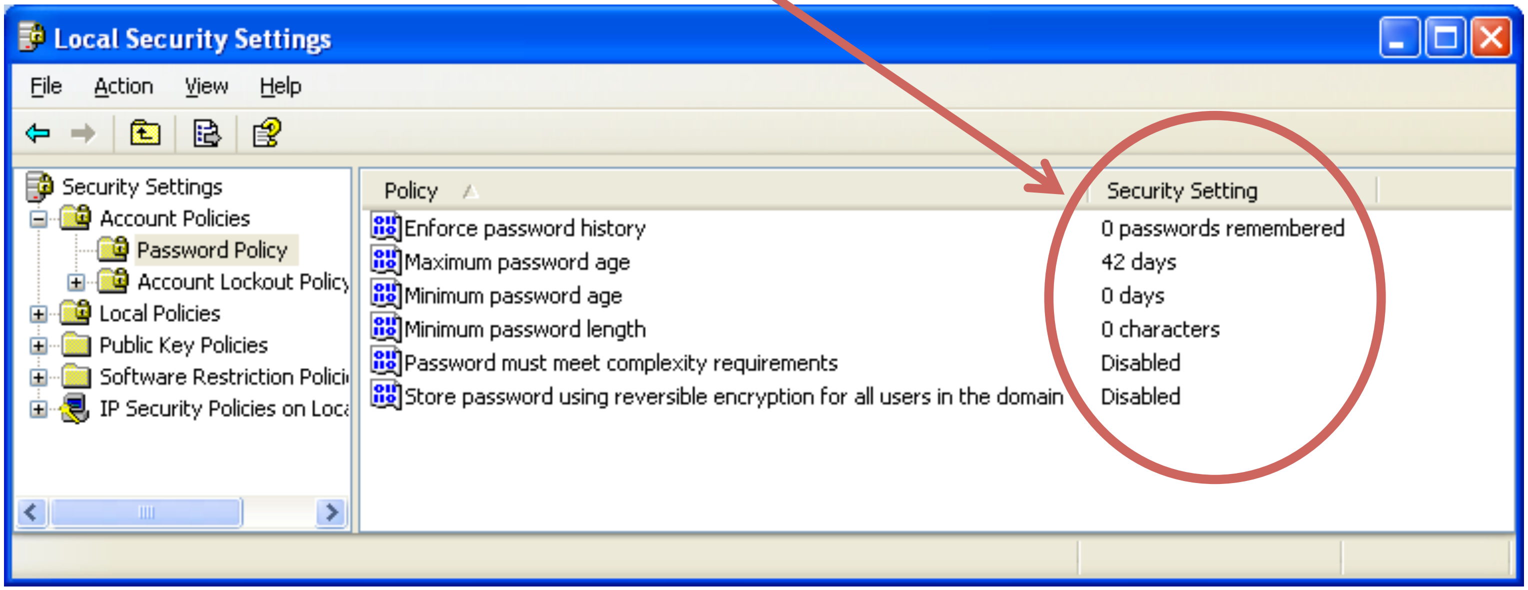
- User Access Reviews: Regularly re-validating all users' access levels on all systems
- This helps prevent:
  - Excessive levels of access
  - Terminated users
  - Potential process problems
- It's a good catch-all detect control

Authentication

- Authentication – How do we know that you are you? We use a combination of the following:
  - Something you know: Passwords
  - Something you have: ID cards, RSA tokens, etc.
  - Something you are: Fingerprints, Retinal Scans, etc.
- Passwords are the most common form
- Desired password controls:
  - Construction (use of alpha, numbers, and special characters) – Example: Esil4&3kc3!
  - Length (six is usually okay, eight is strongly recommended)
  - History

Testing Password Controls

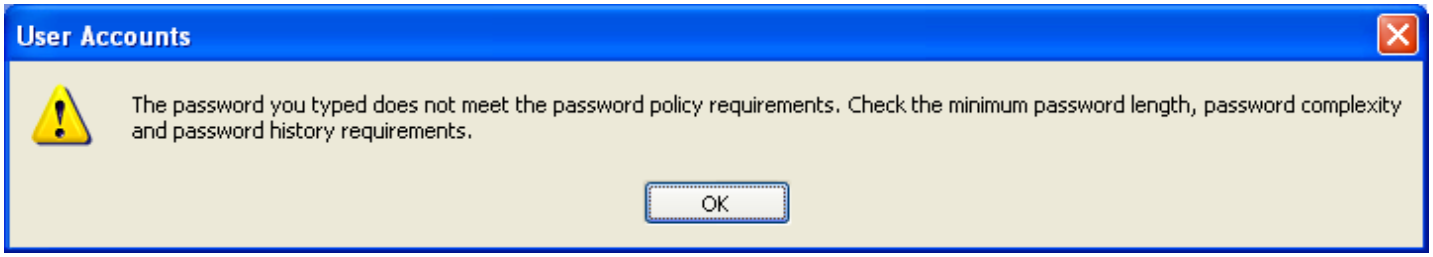
- They are automated controls
- Use ‘test of one’ approach outlined in first session
  - Check the configuration:



Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store password using reversible encryption for all users in the domain	Disabled

Testing Password Controls

- Try changing the password:
  - With a weak password (hopefully getting an error message)

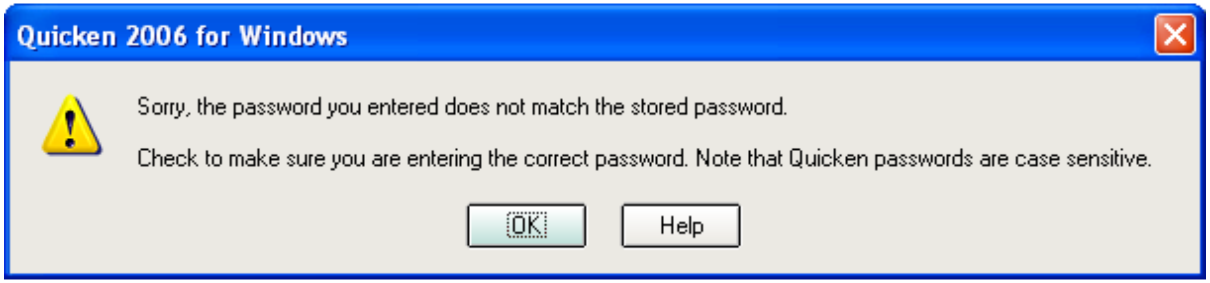


The password you typed does not meet the password policy requirements. Check the minimum password length, password complexity and password history requirements.

  - With a strong password

Testing Password Controls

- Try to log onto the system
  - Failed login attempt (hopefully getting an error message)



Sorry, the password you entered does not match the stored password.

Check to make sure you are entering the correct password. Note that Quicken passwords are case sensitive.

  - Successful login

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"

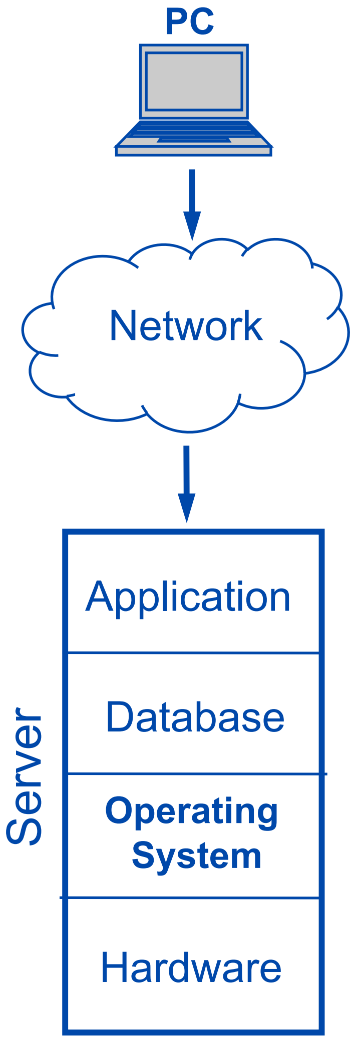
Myth Busted!

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

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

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.



ISACA®
Serving IT Governance Professionals
San Francisco Chapter

When To Bring In "The Experts:"
IT Operations

- Main Focus Is On Availability of Systems and Data:
  - 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

Resources

- Information System Audit & Control Association (ISACA):
  - www.isaca.org
  - www.isaca.org/COBIT
  - www.sfisaca.org
- IT Audit Forum Newsgroup:
  - http://groups.google.com/group/it-audit-forum
- Central Indiana Info Systems Audit & Control Newsgroup:
  - https://lists.purdue.edu/mailman/listinfo/cisaca-l
- Audit Programs and Other Useful Audit Resources:
  - www.auditnet.org
  - http://www.auditnet.org/karl.htm

Any Unanswered Questions?