Intro to IT Auditing for Non-IT Auditors

Steve Shofner, CISA, CGEIT

Senior Manager, Armanino LLP

Core Competencies – C11/12

ISACA®

Trust in, and value from, information systems

San Francisco Chapter

Learning Objectives

Part 1 (C11): Audit Basics & Automated Controls

- Level-Set Our Understanding Of Key Term's & Concepts
- Understand The Role Of Automated Controls In Business Processes
- Audit Process & Required Documentation
- Types Of Automated Controls and Automated Control Test Strategy

Learning Objectives

Part 2 (Session C12)

- The Relationship between Financial/ Operational Controls and IT General Controls (a.k.a. “Why IT General Controls Are Important”)
- Understanding IT General Control Processes & Related Test Strategies
- Knowing When to Bring in ‘The Experts’ (When Things Get Really Technical)

Learning Objectives

- Explain the Relationship between Financial / Operational Controls and IT General Controls (a.k.a. “Why IT General Controls Are Important”)
- Describe Understanding IT General Control Processes
- How to Test IT General Controls
- Knowing When to Bring in ‘The Experts’ (When Things Get Really Technical)

Housekeeping Items

- Please turn cell phones off
- Please close laptops unless you are using them for this session
- Excessive absence(s) will affect CPEs provided

LEVEL-SET UNDERSTANDING OF KEY TERMS & CONCEPTS

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

What Is An Audit?

- An evaluation of business processes (including IT processes) to determine their effectiveness
- Processes contain **risks** that the process's 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 potential for loss (financial or operational)
- What Is An Objective?
  - The purpose 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
  - Existence or Occurrence
  - Completeness
  - Valuation or Allocation
  - Rights & Obligations
  - Presentation & Disclosure
- IT & Operational Objectives
  - Security
  - Availability
  - Confidentiality
  - Integrity
  - Scalability
  - Reliability
  - Effectiveness
  - Efficiency

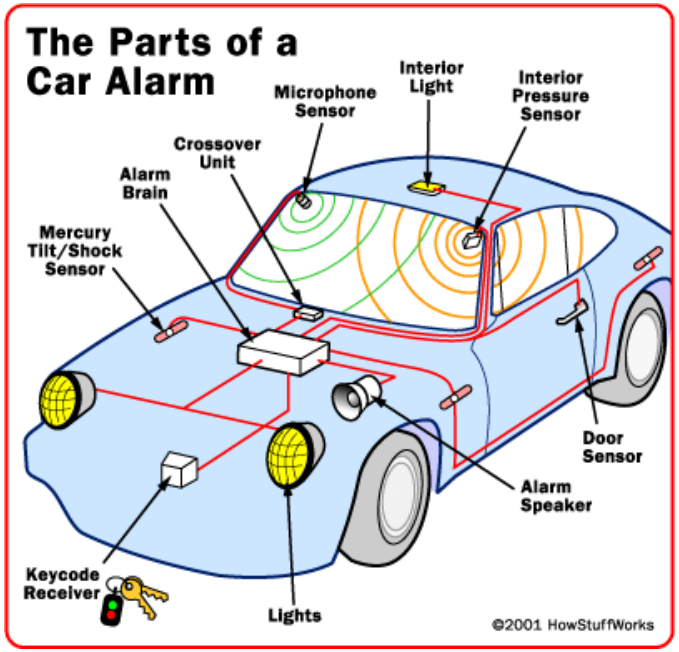
Compliance Audits Could Include Objectives From Both

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

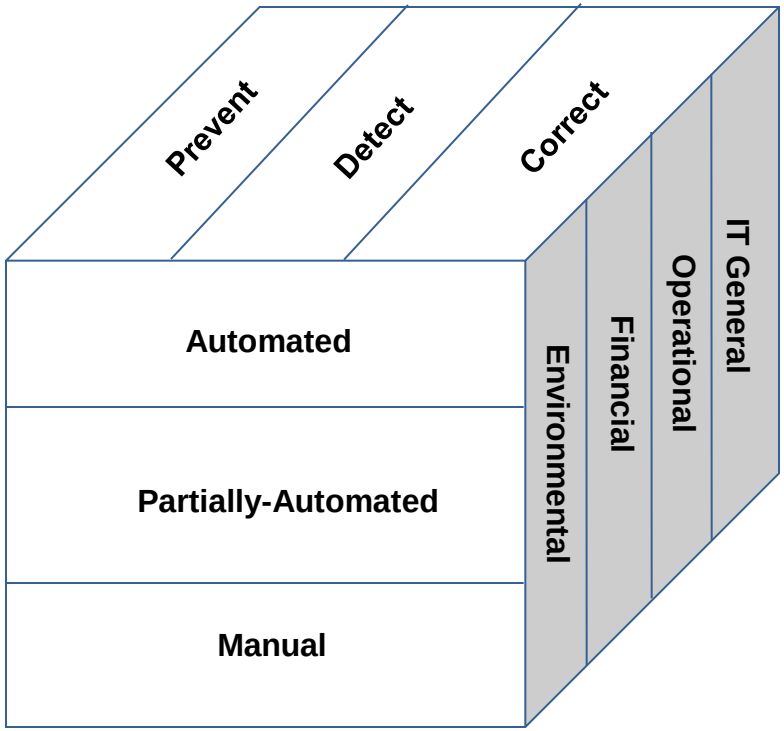
- Prevent Controls
  - The locks on your car doors
- Detect Controls
  - Your car alarm
- Correct Controls
  - Your auto insurance
  - A LoJack system (a device that transmits a signal used by law enforcement to locate your stolen car)



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



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

(note the different types of 'transactions')

Quiz #1

- Classify the controls in the handout

UNDERSTANDING THE ROLE OF AUTOMATED CONTROLS IN BUSINESS PROCESSES

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

Polling Question #1:

- True or False?
  - "IT Controls are too technical – I don't understand what they do"

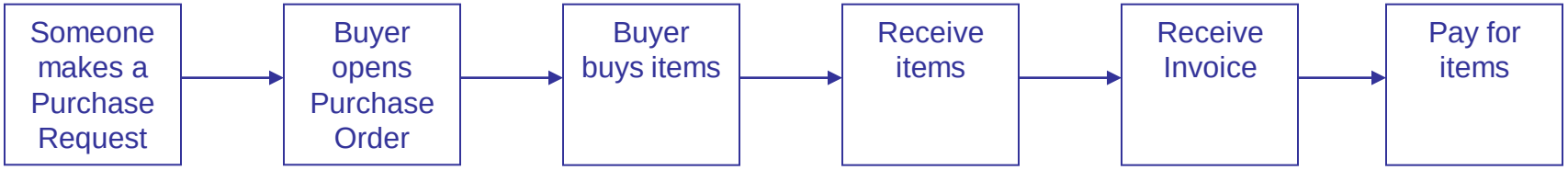
(Answer will be given at the end of this segment)

Introduce Case Study

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

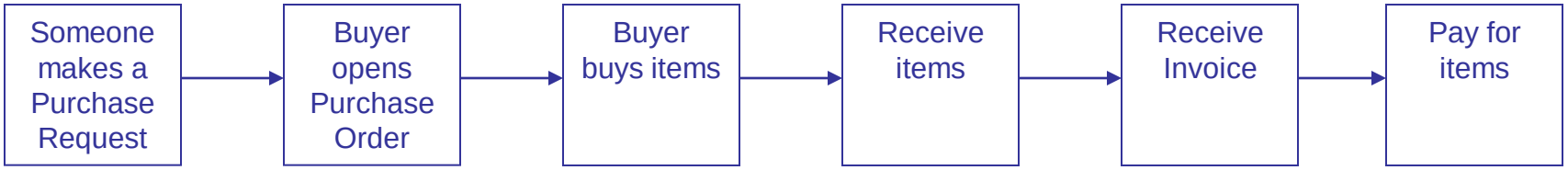
A Made-Up Illustrative Example Only

Purchase To Pay Process



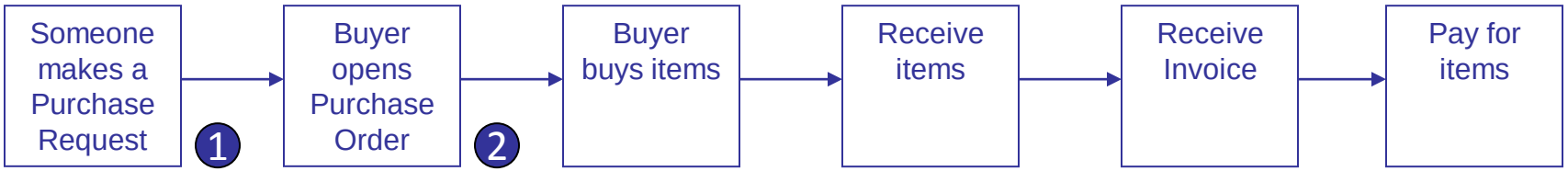
- Financial Objectives
  - Existence or Occoccurrence
  - Completeness
  - Valuation or Allocation
  - Rights & Obligations
  - Presentation & Disclosure
- IT & Operational Objectives
  - Security
  - Availability
  - Confidentiality
  - Integrity
  - Scalability
  - Reliability
  - Effectiveness
  - 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

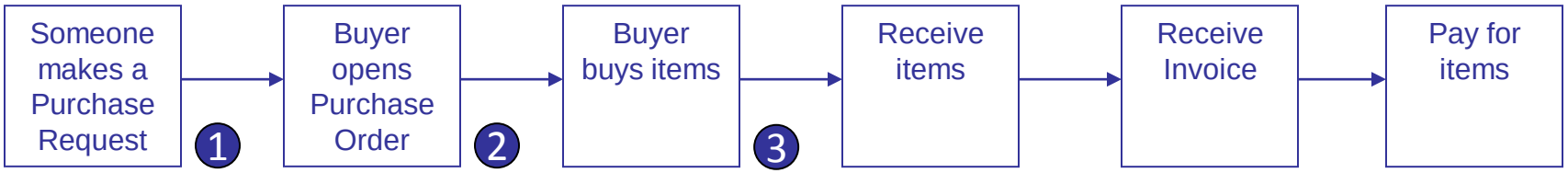
Purchase To Pay Process



- 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

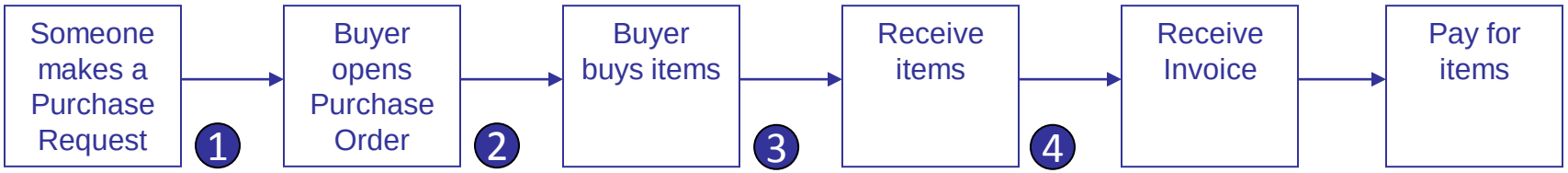
Purchase To Pay Process



- Risk:
  - Buyer may not use approved vendor (gaining the benefit of negotiated volume discounts)
- Control:
  3. Goods can only be purchased from vendors who have been pre-approved

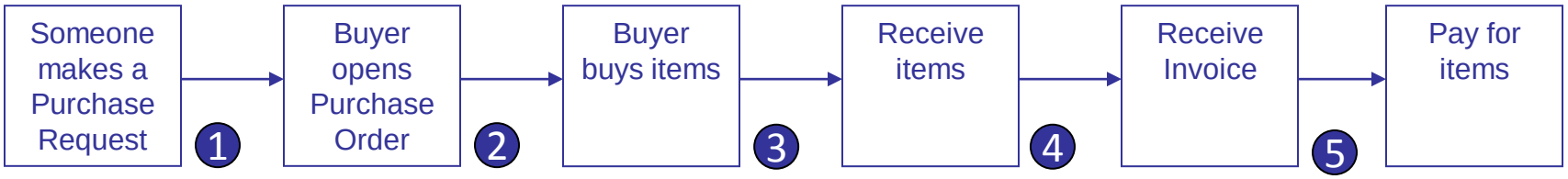
(Assumption: process is in place to approve vendors, and is operating effectively)

Purchase To Pay Process



- Risk:
  - Duplicate or missing items may be received
- Control:
  4. Receiving Clerk counts all items received, ties them to shipping slip, and will only receive complete shipments

Purchase To Pay Process

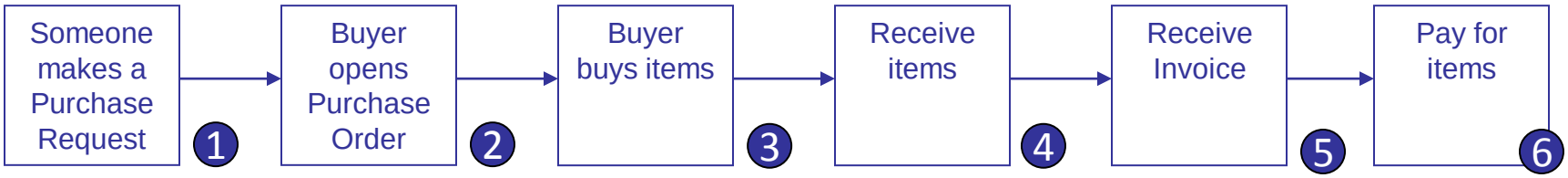


- Risks:
  - Invoice information may not be correct
  - Duplicate or missing invoices may be received
  - Incorrect payment amount

- Controls:
  5. AP Clerk prepares a voucher package, including:
     - Purchase Order
     - Shipping Slip
     - Invoice
     - Check (Payment)

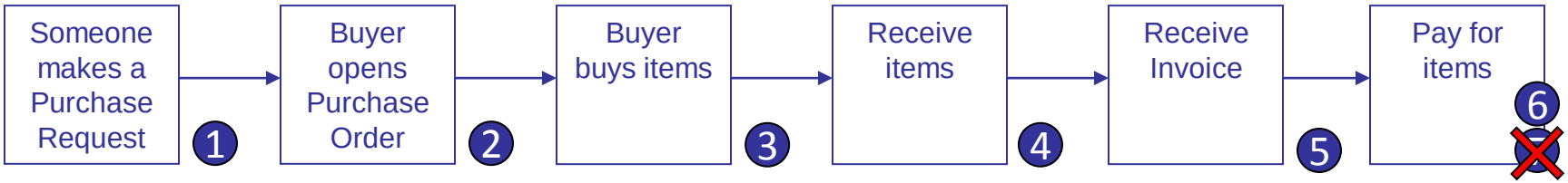
     AP Clerk ties out all information across three documents to ensure completeness & accuracy

Purchase To Pay Process



- Risks:
  - Payment sent to wrong address
  - Wrong payee on check
  - Check may not be signed
- Control:
  6. 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
- Control:
  - ???

Comparison: Manual vs. Automated

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 only allows authorized approvers to approve
Goods can only be purchased from vendors who have been pre-approved	Buyer only purchases from list of approved vendors	PO system provides limited 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: Manual vs. Automated

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

Quiz #2

- For each of the objectives in the handout, create:
  - A manual or partially-automated control, and
  - An automated control

Revisit Polling Question #1:

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

  - A: Automated controls don’t accomplish anything that people weren’t already doing.

AUDIT PROCESS & REQUIRED DOCUMENTATION

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

Testing

- Four Basic Steps:
  - Understand The Process
  - Perform A Walkthrough
    - To exercise process of requesting and gathering evidence
    - Through review of the evidence, confirm and/or complete your understanding of the process being audited
  - Perform Testing
  - Report Results / Findings

Understand The Process

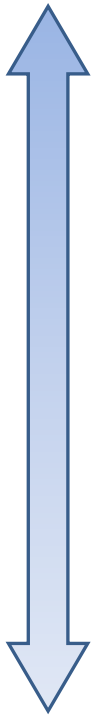
- …Through Reviews Of Documentation And Interviews With Related Personnel
- Document Your Understanding Of The Process And Related Controls in **Narratives**
  - Different than policy, procedure, & standard documents (although, those documents can be leveraged)
  - At a minimum, Narratives should include:
    - Background Information
    - Description of Controls
    - Information Necessary For Testing Controls (Who, What, Where, Why, When, How)
  - Document for testing purposes only…that is all you want

Perform Walkthroughs & Testing

- Perform **Walkthroughs**: A "Test of One"
  - Confirms Your Understanding Of Controls
  - Allows you to identify any problems in pulling populations or samples
- Complete **Testing** & Document Your Work
  - Four Basic Sections
    - Objective
    - Procedures
    - Results
    - Conclusion

Evidence

- Seven types:
  - Confirmation
  - Reperformance
  - Recalculation
  - Analytic Procedures
  - Inspection
  - Observation
  - Inquiry



Stronger Evidence

Weaker Evidence

Inquiry alone is not acceptable.

Report Results / Findings

- **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?
  - *Optional 4th Section: Management's Response*

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, and
  - 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 additional information that is not included or specifically identified in your testing documentation

AUTOMATED CONTROL TEST STRATEGY

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

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 test of many**

Polling Question #2:

- True or False?
  - "Automated Controls are too technical – I don't understand all the technical stuff required to test them"

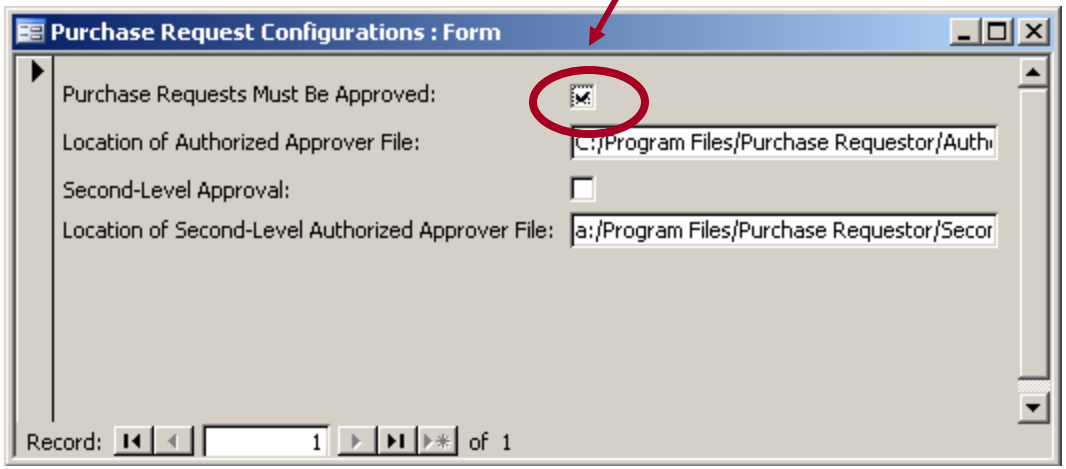
Automated Controls: Test Strategy

- Determine the programmed logic
  - Usually a configuration setting
  - Sometimes setting is “unconfigurable” (programmed into the application, and cannot be changed without changing program code)
- 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:
  - All Purchase Requests must be approved by a Manager or above

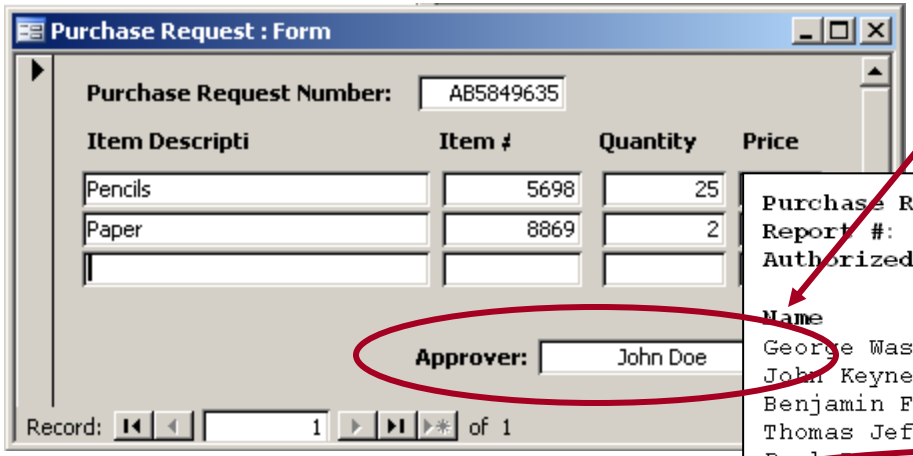
1. Get a screen-shot of the configuration setup screen showing this control is configured:

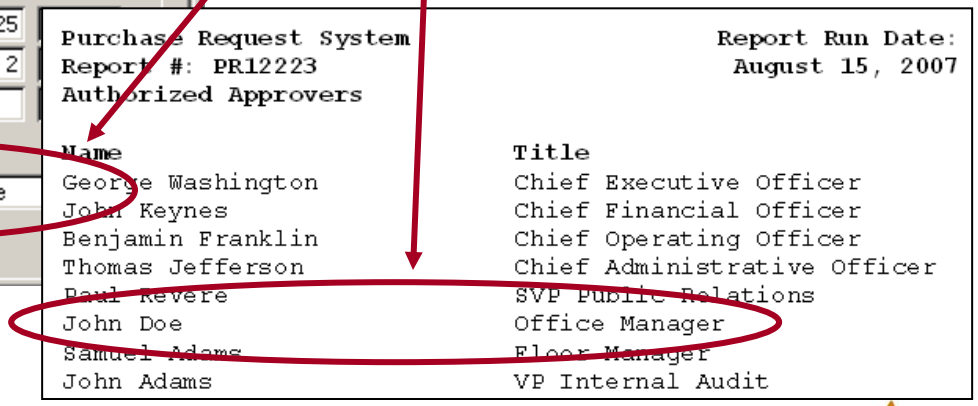


Automated Controls: Test Strategy

- Example:
  - 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.





Automated Controls: Test Strategy

- Example:
  - 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!

Revisit Polling Question #2:

- Q: “Automated Controls are too technical – I don’t understand all the technical stuff required to test them”

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

Checkpoint

- Covered so far:
  - Level-Set Our Understanding Of Key Term's & Concepts
  - Understand The Role Of Automated Controls In Business Processes
  - Audit Process & Required Documentation
  - Types Of Automated Controls and Automated Control Test Strategy

- Coming up (next session)
  - How To Test Common IT General Controls (In A Simple Environment)
  - Knowing When To Call 'The Experts'

Learning Objectives

- Part 1 (Session C11)
  - Level-Set Our Understanding Of Key Term's & Concepts
  - Understand The Role Of Automated Controls In Business Processes
  - Audit Process & Required Documentation
  - Types Of Automated Controls and Automated Control Test Strategy

Learning Objectives

- Part 2 (Session C12)
  - The Relationship between Financial / Operational Controls and IT General Controls (a.k.a. “Why IT General Controls Are Important”)
  - Understanding IT General Control Processes & Related Test Strategies
  - Knowing When To Bring In ‘The Experts’ (When Things Get Really Technical)

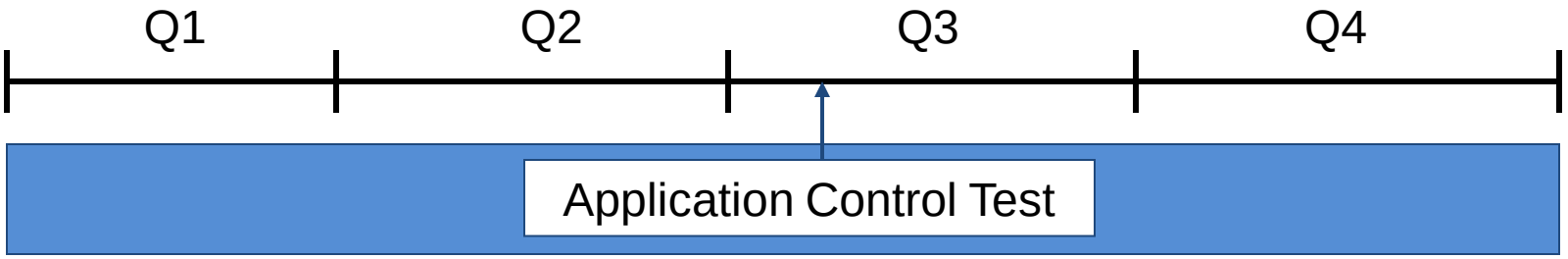
THE RELATIONSHIP BETWEEN FINANCIAL/OPERATIONAL CONTROLS AND IT GENERAL CONTROLS (A.K.A. "WHY IT GENERAL CONTROLS ARE IMPORTANT")

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

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"

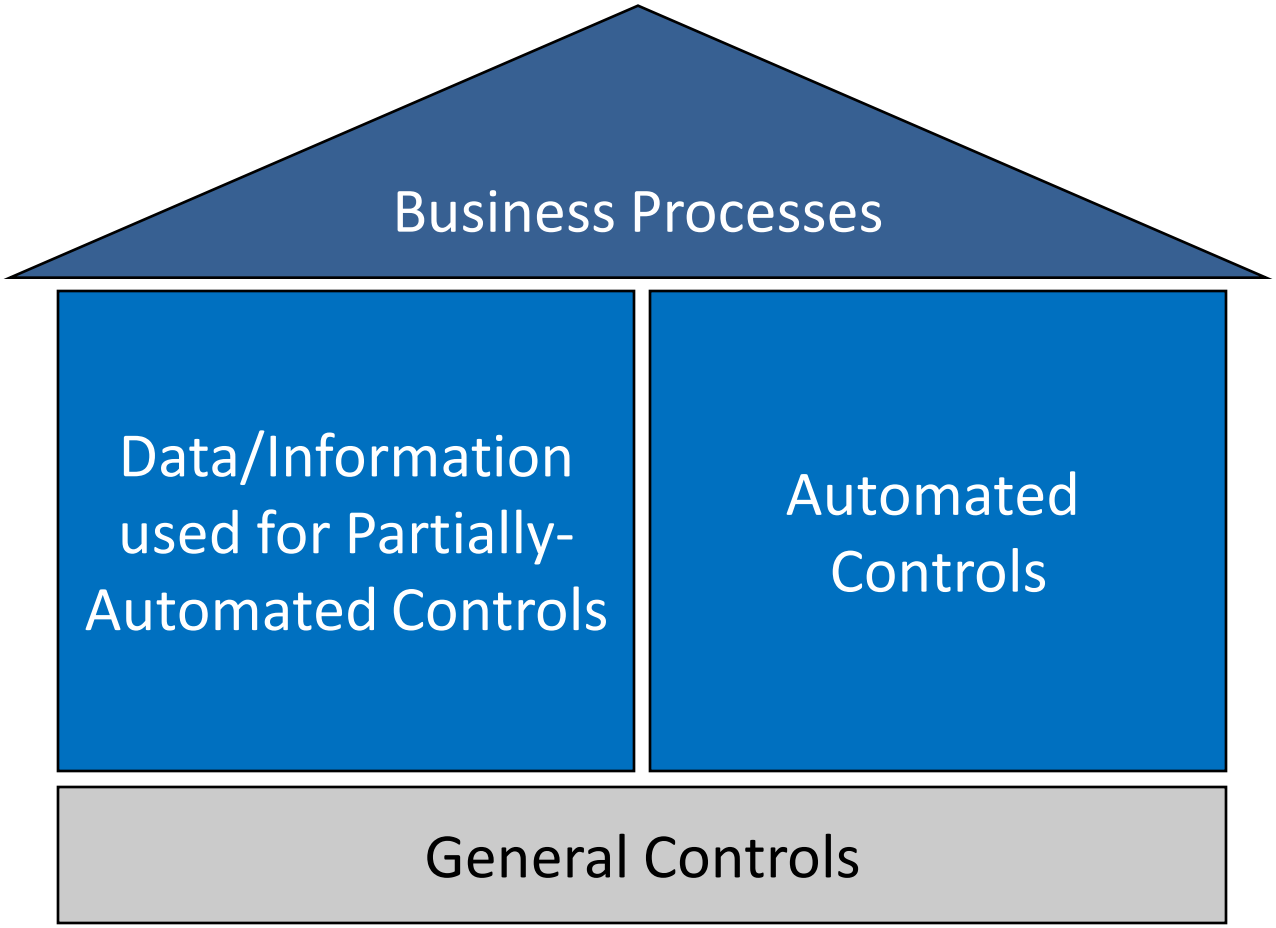


IT General Controls

IT General Controls

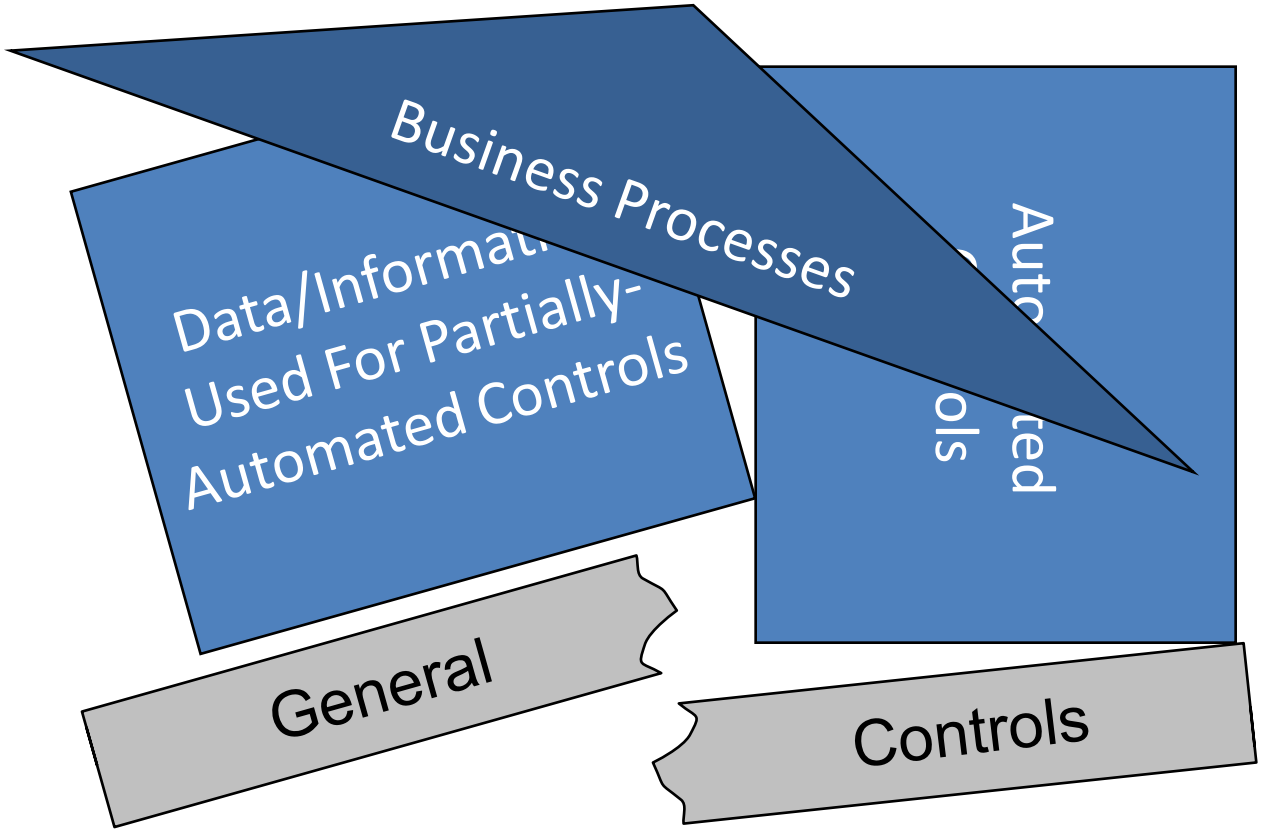
- ★ Change Management
- ★ User Administration
- IT Operations
- Physical Environment

Effective General Controls



Without Effective General Controls

Potential For Significant Problems Exists



Polling Question #3:

- "IT General Controls is all technical stuff...completely out of my realm. I don't understand the technology, and therefore am not qualified to test them"

UNDERSTANDING IT GENERAL CONTROL PROCESSES & RELATED TESTING STRATEGIES

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

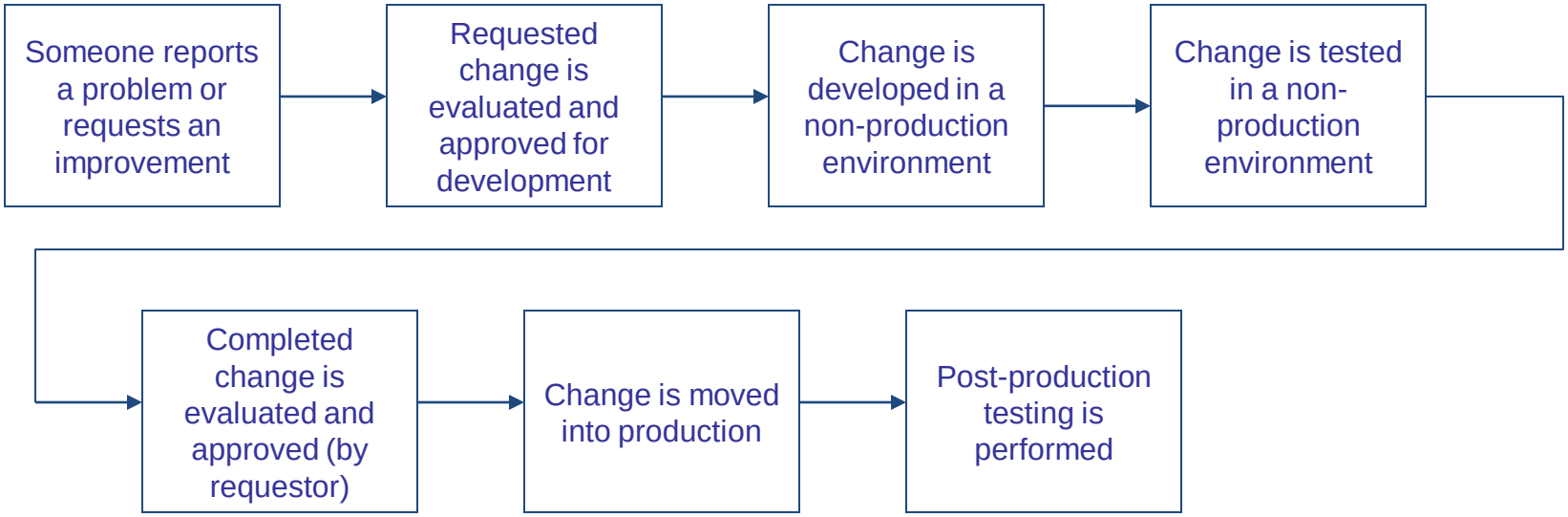
IT Change Management

- 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 (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

User Administration

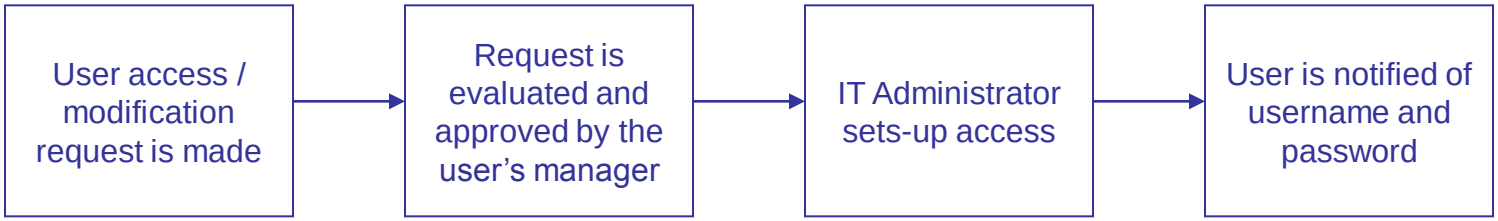
- Processes to:
  - Add user access
  - Modify user access
  - Remove user access

  } 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 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

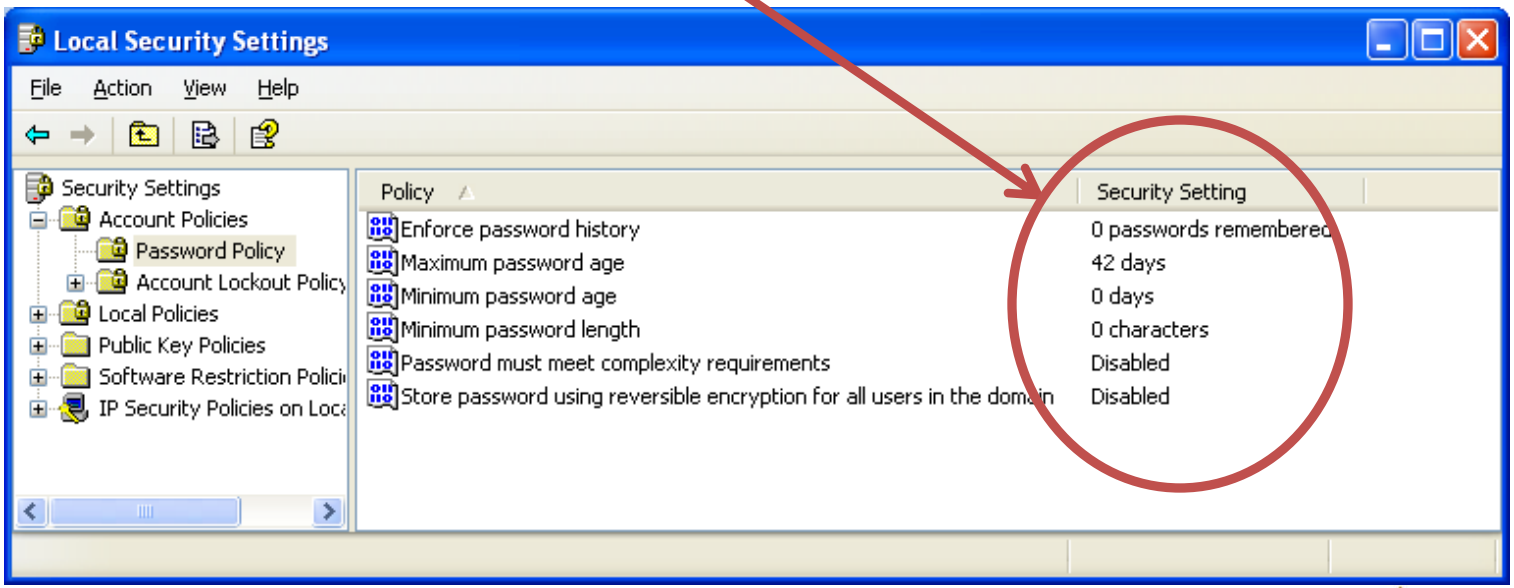
- User Access Reviews: Regularly re-validating all users' access levels on all systems
- This helps prevent:
  - Excessive levels of access
  - Terminated users
  - Potential process problems
- It's a good catch-all detect control

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 can be okay in some situations; eight is strongly recommended)
  - History

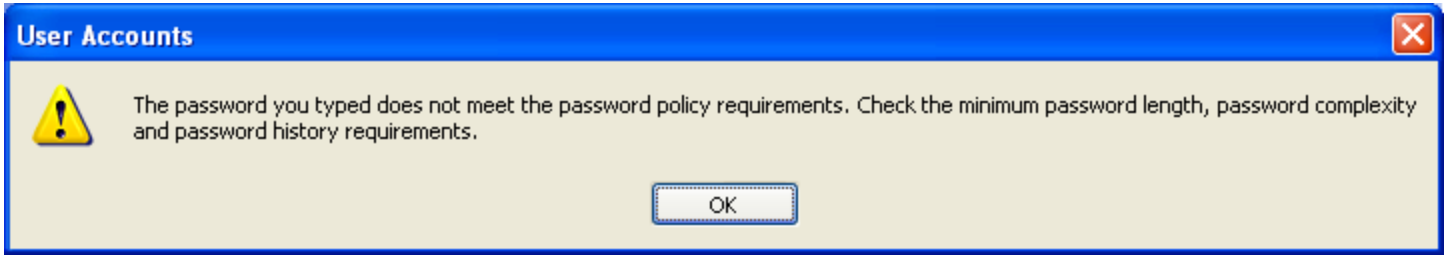
Testing Password Controls

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



Testing Password Controls

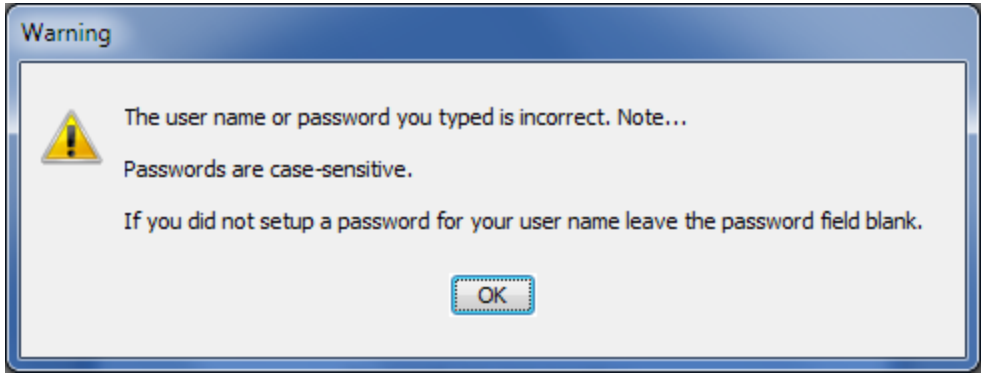
- Try changing the password:
  - With a weak password (hopefully getting an error message)



  - With a strong password

Testing Password Controls

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



  - Successful login

Revisit Polling Question #3:

Q: “IT General Controls is all technical stuff...completely out of my realm. I don’t understand the technology, and therefore am not qualified to test them”

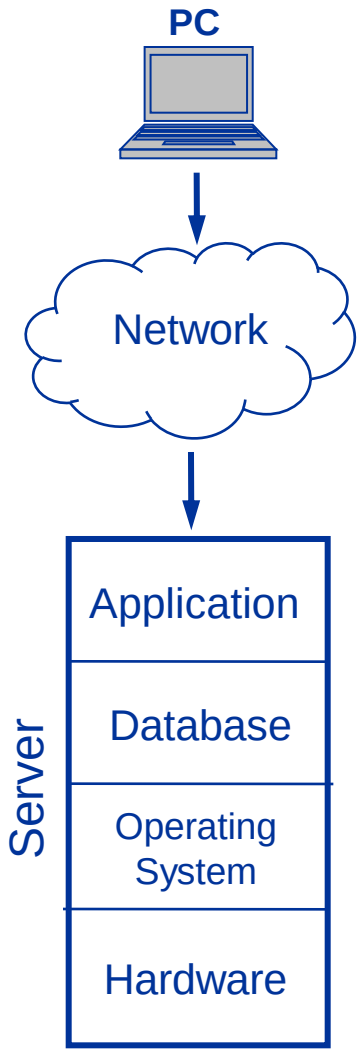
A: These processes are people-driven and non-technical. You *can* test them.

UNDERSTANDING WHEN TO CALL IN 'THE EXPERTS' (WHEN THINGS GET REALLY TECHNICAL)

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

When To Bring In "The Experts"

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



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 Newsgroups:
  - http://groups.google.com/group/it-audit-forum
  - http://finance.groups.yahoo.com/group/ITAuditForum
- 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

Questions?

Steve Shofner, CISA, CGEIT

Senior Manager, Armanino LLP

Steve.Shofner@amllp

925-790-2879

www.amllp.com