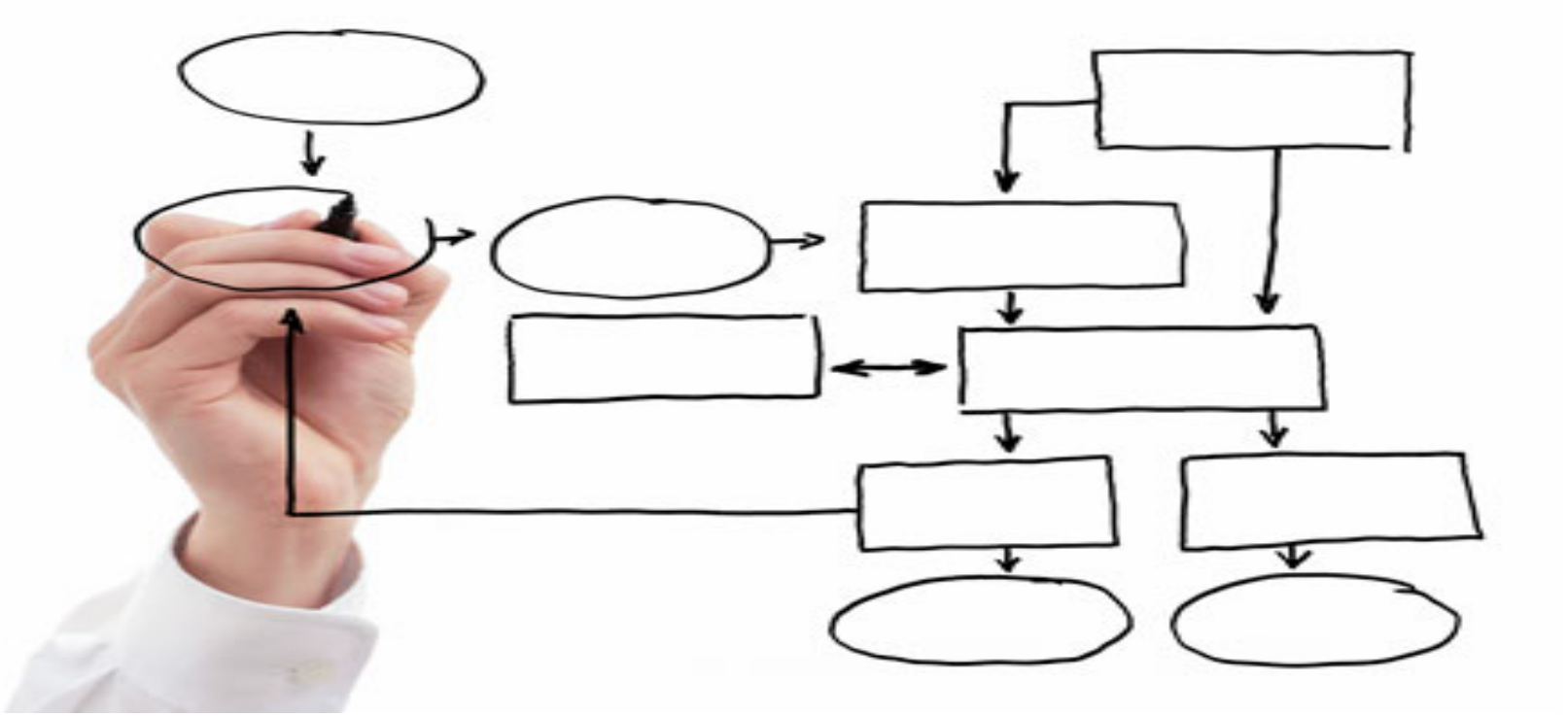


MIS 5121: Business Processes, ERP Systems & Controls
Week 13: *Auditing,* Emergency Access

FOX | MIS
Management Information Systems

Edward Beaver
Edward.Beaver@temple.edu
ff

Special Guests

Kapish Vanvaria

- Ernst & Young
- Manager | Advisory Services
  (assists clients address complex compliance, financial, operational and technology risks)
- Temple MIS Advisory Council

Leanna Baselice

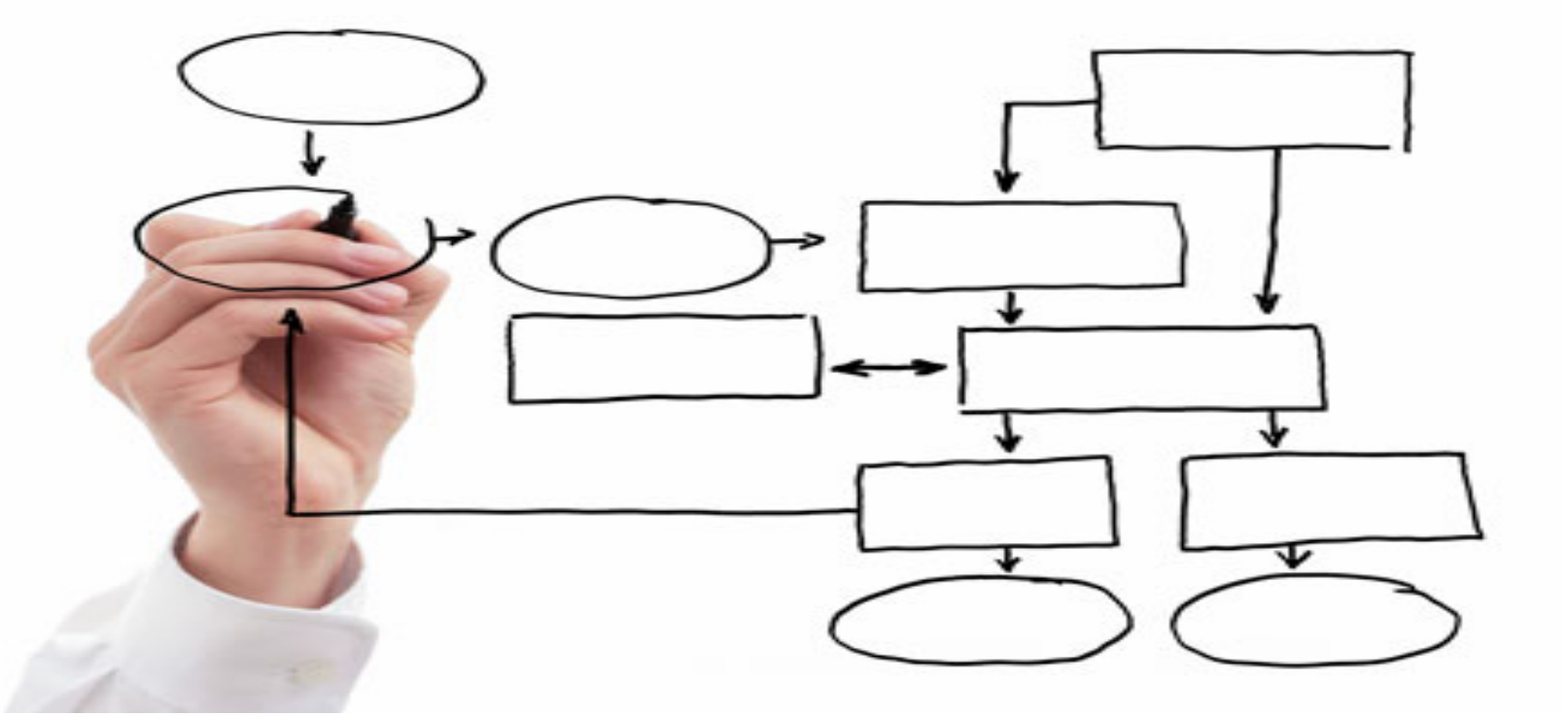
- Ernst & Young
- Firm SAP Expert
- Saint Joseph's Alum

MIS 5121: Auditor's Visit Topics

- What is the most common 'weak' or vulnerable control area?
- How to you define your audit scope for a complex business? How do you organize, define focus?
- What is the most important document to review in an audit?
- Are companies being audited serious about security in SAP?
- What tools is most effective when auditing clients?
- How do you plan the scope of an audit?
- Who are the people they interview during an audit? Who do they interview first?
- What do they audit in an ERP system – what do they look at?
- What are the risk assessment tools they use? Has their assessment of them changed over the years?

MIS 5121 : Auditor's Topics

- Have you personally detected a fraud scenario in your audit? If so, please explain
- How do you maintain your independence? Is that easy?
- Does SAP provide good control environment vs. other systems (ERP, other)?
- Since SAP can be customized in so many ways, how does an auditor know what to audit when everything is different with each client?



MIS 5121: Business Process, ERP Systems & Controls

Real World Control Failures:

By: _Mai Ta_

FOX | MIS
Management Information Systems

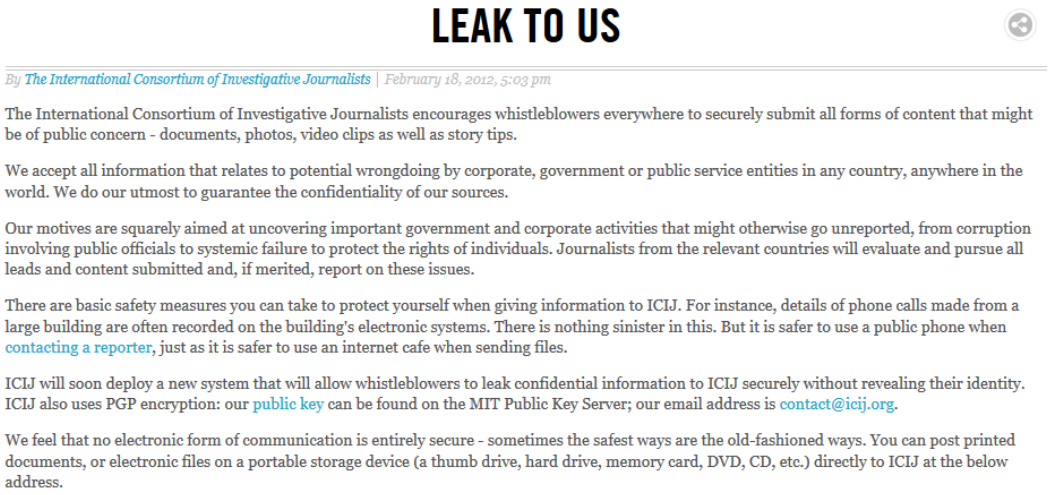
Control Failure:
The Panama Papers

- Background:
  - April 2016, Panama Papers leaked document about 214000 offshore companies
  - 140 politicians from 50 countries
  - More than 500 banks requested offshore companies for clients
  - Law firms and banks sell financial secrecy to politicians, fraudster and drug traffickers
- Control Failures:
  - Data security
  - Tracking ability
  - M&A management
- Results:
  - Political figures resign
  - Mossack Fonseca is investigated by police from countries that MF has presence
  - Investigation on people who was named in the report

Control Failure: The Panama Papers

- What Could / Should those in Authority Have Done Different?:
  - Choosen ethical leaders
  - Tighten laws on opening offshore companies

- What would you choose to do?
  - As manager of a company
  - As a citizen of the world



LEAK TO US

By *The International Consortium of Investigative Journalists* | *February 18, 2012, 5:03 pm*

The International Consortium of Investigative Journalists encourages whistleblowers everywhere to securely submit all forms of content that might be of public concern - documents, photos, video clips as well as story tips.

We accept all information that relates to potential wrongdoing by corporate, government or public service entities in any country, anywhere in the world. We do our utmost to guarantee the confidentiality of our sources.

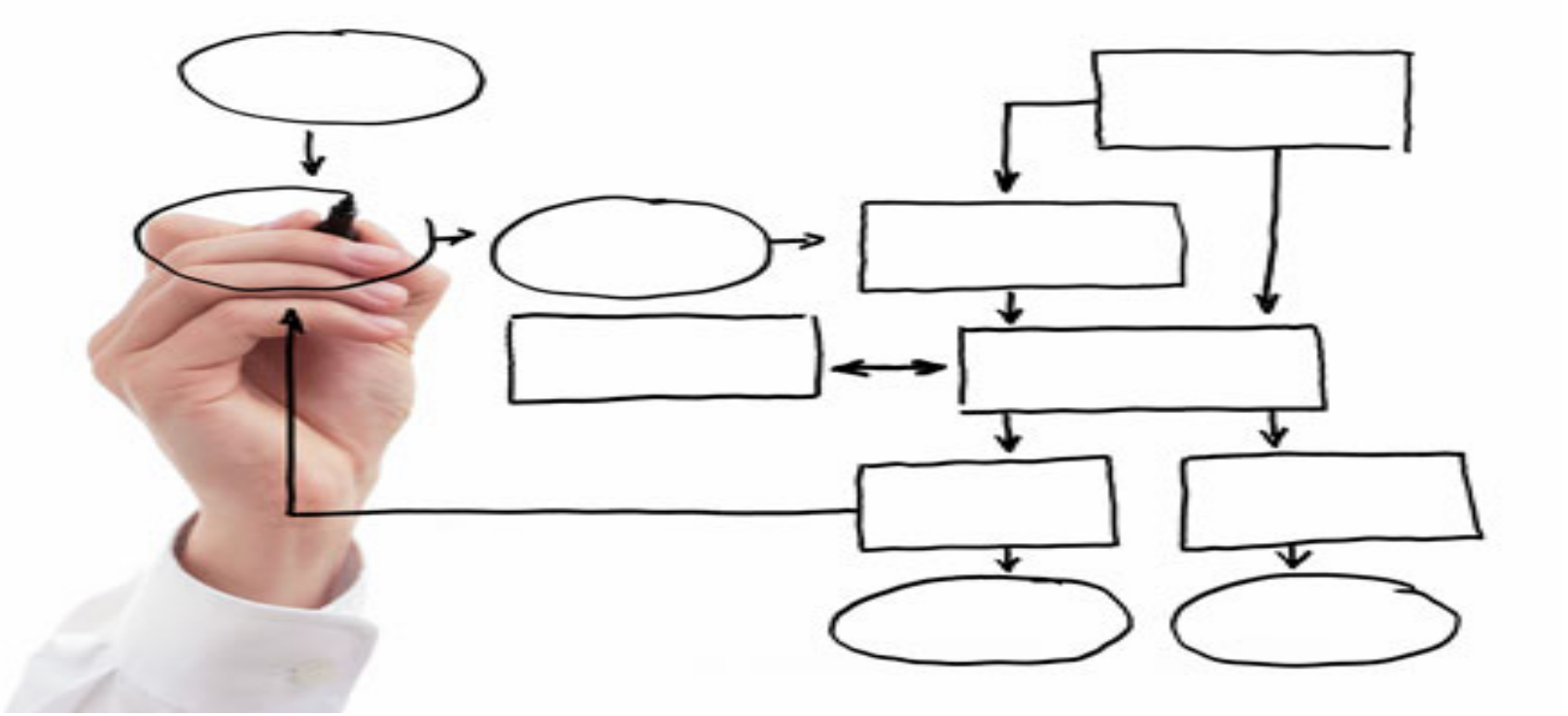
Our motives are squarely aimed at uncovering important government and corporate activities that might otherwise go unreported, from corruption involving public officials to systemic failure to protect the rights of individuals. Journalists from the relevant countries will evaluate and pursue all leads and content submitted and, if merited, report on these issues.

There are basic safety measures you can take to protect yourself when giving information to ICIJ. For instance, details of phone calls made from a large building are often recorded on the building's electronic systems. There is nothing sinister in this. But it is safer to use a public phone when contacting a reporter, just as it is safer to use an internet cafe when sending files.

ICIJ will soon deploy a new system that will allow whistleblowers to leak confidential information to ICIJ securely without revealing their identity. ICIJ also uses PGP encryption: our public key can be found on the MIT Public Key Server; our email address is contact@icij.org.

We feel that no electronic form of communication is entirely secure - sometimes the safest ways are the old-fashioned ways. You can post printed documents, or electronic files on a portable storage device (a thumb drive, hard drive, memory card, DVD, CD, etc.) directly to ICIJ at the below address.

- Reference:
  - https://panamapapers.icij.org/
  - http://www.theguardian.com/news/2016/apr/03/mossack-fonsecas-response-to-the-panama-papers



MIS 5121: Business Process, ERP Systems & Controls

Real World Control Failures:

By: Alaa Abuali

FOX | MIS
Management Information Systems

Control Failure: Skimming

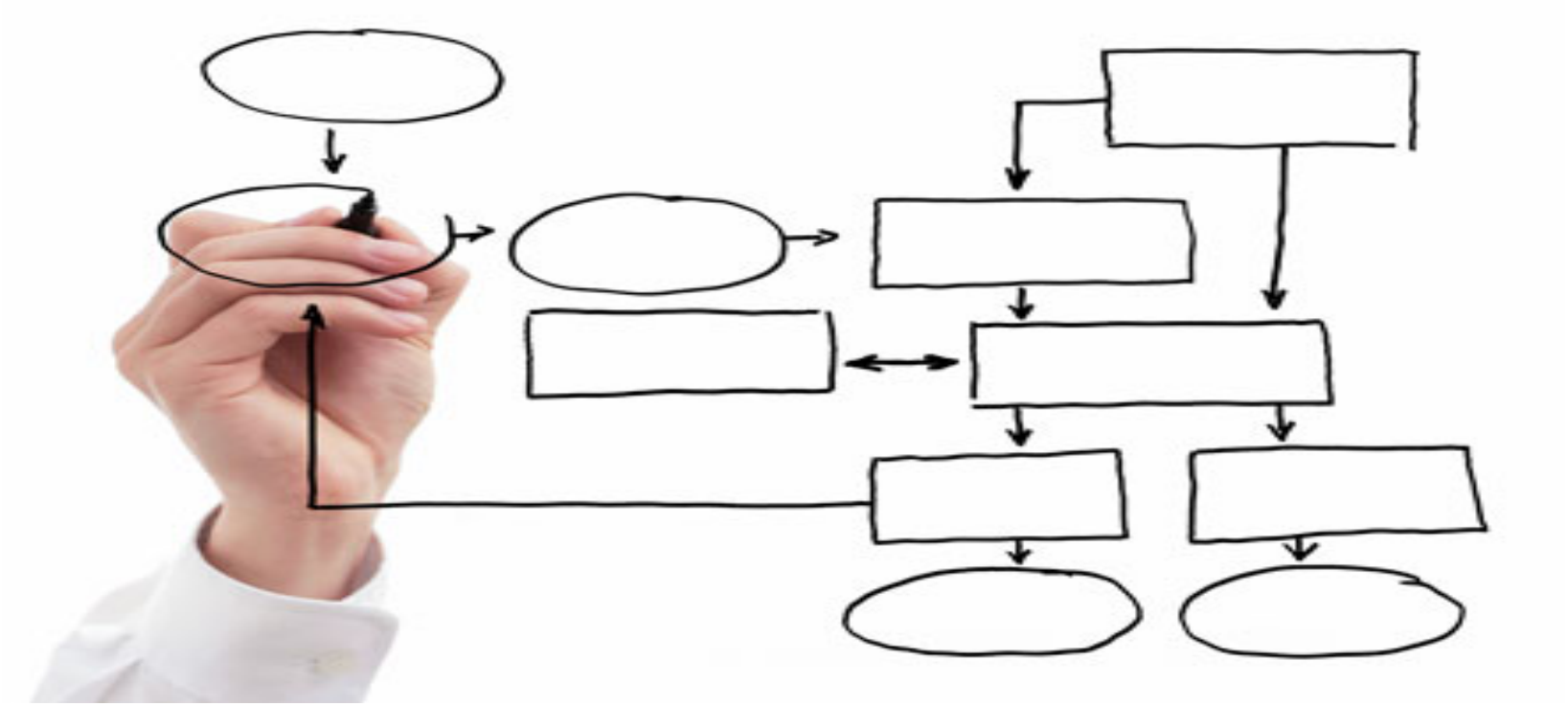
- Background:
  - American Apparel and home goods company, Divisions (T.J Maxx, Home goods, Marshalls, Sierra Trading Post).
  - Jan, 17, 2007 announced hack of computer systems where customer data was stolen affecting 45.7 million customers over a period of 18 months. (biggest intrusion at the time).
  - hackers used multiple techniques to access TJX database.
- Control Failures:
  - Weak encryption technologies used for data transfer
  - no intrusion detection systems in place to sense presence of hackers in systems
  - weak security controls used on instore kiosks allowed hackers to use them as gateways to system
  - Lacked proper processing logs or audit trail in order to conduct proper forensic analysis
  - Failed to meet 9 of 12 payment card industry data security standards related to data encryption, access controls, and firewalls.

Control Failure: Skimming

- Results:
  - TJX data systems were compromised for over 18 months without detection.
  - millions of customers personal information was stolen resulting in significant damage to tjx customers.
  -

- What Could / Should those in Authority Have Done Different?:
  - used up to date security encryption and technology.
  - Improved security policies and procedures.
  - Informed customers immediately after breach was detected.
  -

- Reference:
  - _____ Fraud: http://www.computerworld.com



MIS 5121: Business Process, ERP Systems & Controls

Real World Control Failures:

South Carolina Department of Revenue Security Breach

By: Wen J Chung

FOX | MIS
Management Information Systems

Control Failure: South Carolina Department of Revenue – Security Breach

- Background:
  - SC DOR – Responsible for administering state tax laws and collecting tax from all SC citizens
  - highly sensitive personal identification data. i.e name, DOB, Social security card and etc…
- What happen?:
  - On Oct 10 2012, Informed of cyber-attack involving personal identification of taxpayers
  - Hackers employed the attack through uneducated employees to steal their credential and gain access of the system through email phishing.
  - Injected malware to collect employee's user ID and password, installed a backdoor on one of the DOR server.
  - Stole millions of sensitive personal identification data
- Control Failures:
  - Leadership
    - SC DOR leadership Opted out of the stat's optional intrusion detection monitoring program
    - 1970s technology to safeguard its asset
  - Vulnerabilities
    - Email phishing – send email to DOR employee
    - Compromised employee's computer clicked on the link on the email
    - Injected malware – an automated program to harvest user ID and password information to he hackers
    - Utilize employee credential – Remote access to the DOR computer system

Control Failure: South Carolina Department of Revenue – Security Breach

- Results:
  - Fail to safeguard its most important asset: sensitive data (millions of credit card records was stolen).
  - Incident affected more than three quarters of SC 4.6 million populations
  - Mandiant – hired cyber security expert company to resolve the issue
  - SC DOR – to provide one year credit monitoring
  - Cost the state more than 14 million dollars

- What Could / Should those in Authority Have Done Different?:
  1. Leadership buy-in
  2. Stay current with the newest technology and system upgrade
     - Email filtering software
     - Antivirus software
     - IP monitoring detection system
  3. Strong Security policy by partner with employees
     - Frequent password change and complexity requirement
     - Promote cyber security awareness
       - Training or reward
- Reference:
  - http://www.governor.sc.gov/Documents/Media_Release_10262012.pdf

Segregation of Duties

Definition

'ensuring that at least two individuals are responsible for the separate parts of a task'

Goal: prevent error and fraud

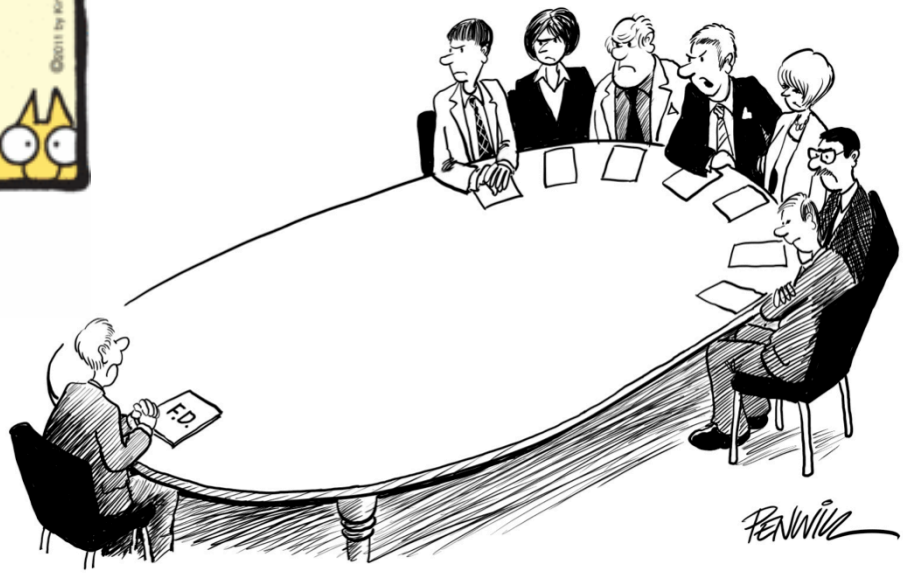
Segregation of Duties

Implementation

- Break down tasks that might reasonably be completed by a single individual into multiple tasks
- No one person is solely in control
- Prevent one person from having 2 of:
  - access to / Custody of assets (operational responsibility)
  - Responsibility for asset's accounting / reconciling
  - Approval
- Prevent opportunity to commit and hide errors, fraud, theft

Success with Internal and External Auditing
My Personal Experience

"It went pretty well. The auditor took one look at my files and retired!"



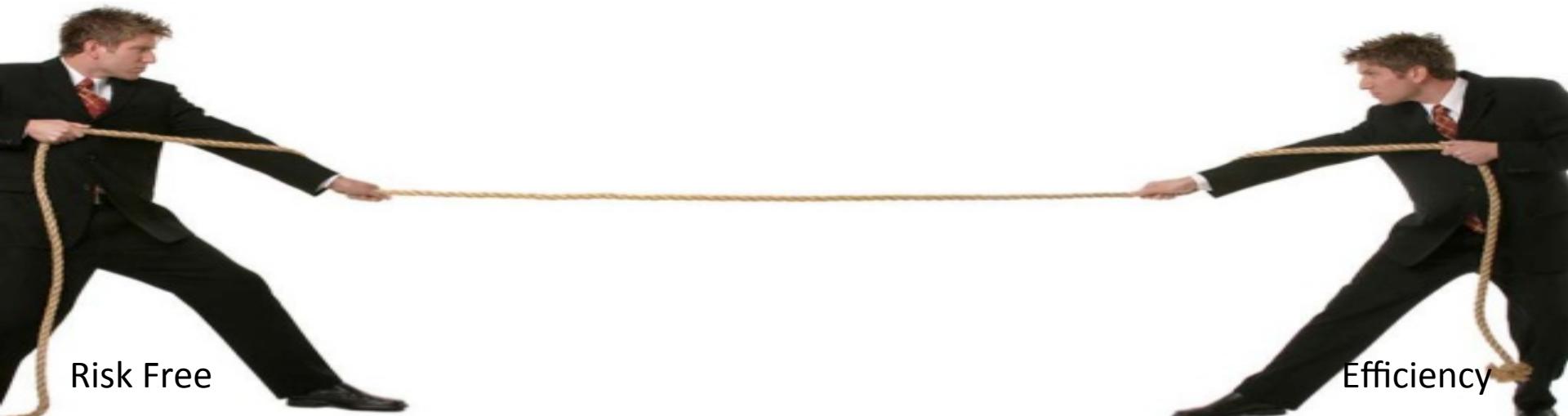
"WE DON'T WANT YOU TO VIEW THIS AUDIT COMMITTEE AS BEING IN ANY WAY CONFRONTATIONAL"

Success with Auditors

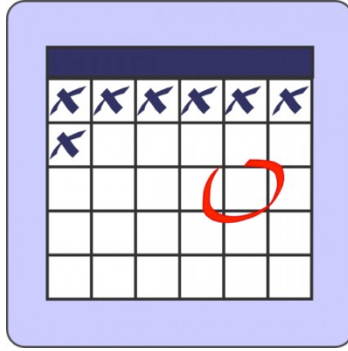
- Have Strong / Deep Knowledge
  - Process
  - Business / real world scenarios
- Able to Master the Details
- Understand Auditor perspectives
  - Job / Role to accomplish
  - Risks
  - Vocabulary

Success with Auditors

- Work Cooperatively
  - Balance the Tension: Know which side you're on and be an effective counter-weight
  - Focus on what's "best" for the organization



MIS 5121: Upcoming Events



- Reading Assignment 8 – *Due: Yesterday*
- Reading Assignment 9 – *Due: April 24*

- Guest Lecture: Auditor's Perspective - *Today*

- Guest Lecture: SAP What's New (HANA) - *April 25*

MIS 5121: SAP Visit Questions

- _____
- _____
- _____
- _____
- _____
- _____
- _____
- _____
- _____

System and Integration Controls

Key Information Technology Risks

- System Security
- Data Migration
- Data Interface
- Change Management
- Transport Security
- Instance Profile Security
- Table Security
- Data Dictionary, Program and Development Security
- Logs and Traces
- **Firefighter access**
- **Powerful User ID's and Profiles**
- Background Processing (Batch vs. foreground: real-time)

Powerful User ID's and Profiles

Powerful User ID's and Profiles

SAP created these powerful ID's and access profiles. However they must be caged and controlled.

SAP_ALL

- Composite profile containing all SAP authorizations
- Users with this profile can perform **all** tasks within SAP
- Concern with use even by administrators – Distribute the responsibility and authority

SAP_NEW

- Grants **all** authorizations when system is upgraded and new authorization objects are introduced
- Assign new authorizations to user's as needed and remove SAP_NEW from all roles

Risk and Recommendation
Powerful Profiles

Risks:

- SAP_ALL profile provides full access to the system
  - Contains * for authorizations
- SAP_NEW is an upgrade profile
  - Composite Profile contains Simple Profiles for each new release

Recommendations:

- No User should have SAP_ALL or SAP_NEW in Production (PRD) & QA
  - Basis, Security and other support personnel should not have SAP_ALL or SAP_NEW]
  - Interface and System IDs should sue custom roles (not SAP_ALL, SAP_NEW)
- Very limited (if any) Users should have SAP_ALL or SAP_NEW in Dev
  - Basis may need Dev access to SAP_ALL on occasions

Risk and Recommendation
Powerful ID's

Risks:

- SAP* is a super user ID
  - Included with System
  - Assigned the powerful SAP_ALL profile

Recommendations:

- Change SAP* user ID password in all clients
- Lock SAP* and monitor unauthorized access attempts
- Change system parameter LOGIN/NO_AUTOMATIC_USER_SAPSTAR to 1
  - Deactivates the special default properties of SAP* (e.g. removes the ability to login to a client with a password of PASS if SAP* user master record is deleted from that client)

Note: SAP*user master record should not be deleted

SAP Default IDs

- Predefined User IDs and passwords in all SAP installations
- Need to be protected with password changes

DDIC

- Special privileges for software logistics and ABAP/4 dictionary
- Auto-created when clients 000 & 001 created for installation and setup tasks (Do not delete DDIC master record in Client 000)

SAPCPIC

- Allows the SAP system to call programs and function modules
- Cannot log on in dialog
- Allows EarlyWatch to collect performance data, execute external background programs

EarlyWatch

- Used for the Performance Monitor
- Change initial password in client 066

Risk and Recommendation

SAP Default IDs

Risks:

- Unauthorized users can gain access to the system if default passwords for SAP-delivered standard users are not secure

Recommendations:

- Develop Policies and Procedures for their usage and monitoring
- Change default passwords for all these ID's for all clients in PRD
- Run report program RSUSR003 (via SE38/SA38) details of default password and locked status

……

Emergency / Firefighter Access

Firefighter / Emergency User

Would you permit this Person into your home?

Firefighter / Emergency User

What about in an emergency??

Firefighter (FF) / Emergency User

- Enables users (typically support) to perform duties not included in roles or profiles assigned to their user IDs (least privilege)
- Emergency, special situations:
  - Need change/update authorization in production system to fix critical problems
  - Duplicating Real world transaction use to diagnose / troubleshoot
  - Verifying Production data
  - Check production system performance
  - Sometimes critical transactions require developer assistance to resolve issues in production environment.
- SuperUser Privilege Management (SAP GRC term)

Firefighter (FF) / Emergency User

- Each Firefighter ID (Give the FF the Key):
  - Has specific authorization rights (Best practice is to distribute access among several different types of IDs – e.g. OTC, Planning, P2P)
  - Access Is pre-assigned to specific users
  - Access has a validity date.
- FF provides this extended capability while creating an auditing layer to monitor and record Firefighter usage (Key use logs)
  - Reason for emergency use
  - Date / time stamps
  - What Transactions were used
  - Which updates made

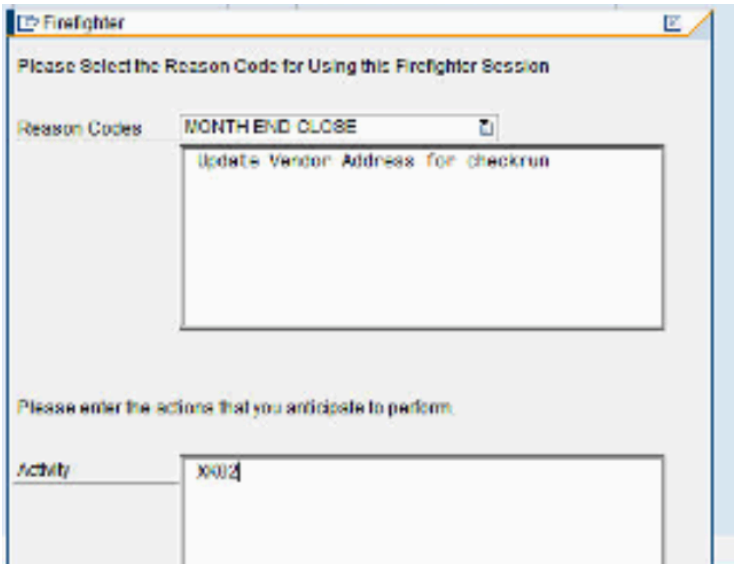
Firefighter (FF) / Emergency User

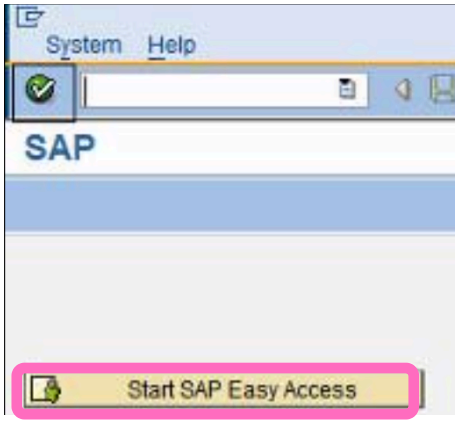
- Access (enter the audit layer first) :
  - ECC Transaction: /n/VIRSA/VFAT
  - GRC Module

- Logging On creates a new SAP session as if the FF ID had logged on.

Firefighter (FF) / Emergency User

- Reason for access:





- Logging On creates a new SAP session as if the FF ID had logged on.

Firefighter / Emergency User

- ‘Best’ Practices
  - Documented FF / Emergency User Policy
  - FF focus is Production (PRD) System / clients (less to QA)
  - Do not give SAP_ALL or equivalent access to FF
  - Create FF ID for each of several useful process / support areas: e.g. (Security, IT Admin, OTC, Planning, P2P)
  - FF Used only for emergencies (not routine use)
  - Regular Support access in PRD sufficient to prevent need for routine FFID Use (good display, SPRO, low risk transactions (e.g. create Delivery))

Firefighter / Emergency User

- 'Best' Practices
  - Access only as there's a valid need – Approval needed
  - Limit access only to time needed (e.g. particular event like 'Go-Live')
  - Assure complete logging of FF Actions (config)
  - Assure audit of all access for (via reports or e-mail notification):
    - Valid Reasons -
    - Special review of all 'changes'

Firefighters Log Report

Download

Firefighter ID / Date	Firefighter / Time	Session Date / Server Name	Session Time / Transaction	Reason Code / Report Name	Report Title
FF_CHECKS	JSMITH	29.06.2007	17:30:33	MONTH END CLOSE	
BACKGROUND JOB WAS NOT SCHEDULED/LOG & FILE NOT YET GENERATED.					
FF_VENDORS	JSMITH	29.06.2007	14:15:16	MONTH END CLOSE	
29.06.2007	14:20:54	iwdfvm2160_ERP_10	XK02	RFC	Change vendor (centrally)
29.06.2007	17:35:46	iwdfvm2160_ERP_13		RFC	
29.06.2007	17:35:49	iwdfvm2160_ERP_13	SMEN	RFC	Session Manager Menu Tree Display
FF_VENDORS	JSMITH	29.06.2007	17:37:00	MONTH END CLOSE	
29.06.2007	17:38:49	iwdfvm2160_ERP_13	SMEN	RFC	Session Manager Menu Tree Display

Firefighter Roles

Role Type	Description
Administrator	Administrators have complete access to Superuser Management capability. They assign firefighter (FF) IDs to owners and to FFs. Administrators run reports, maintain data tables and assure the Reason Code table is current.
Owner	Owners assign FF IDs to firefighters and define controllers. Owners can view the FF IDs assigned to them by the administrator. They cannot assign FF IDs to themselves.
Controller	Controllers monitor FF ID usage by reviewing the log reports, log report workflow and e-mail notification of FF ID logon events. Administrators enable e-mail notification through the Controllers table, which is done in FF Assignment and GRC Configuration.
Firefighter	Firefighters can access all FF IDs assigned to them and can perform any tasks for which the IDs have authorization. FFs use the FF ID logons to run transactions during emergency situations.

Key IT Controls Overview

- Powerful ID's and Profiles
  - 2-3 risks that exist
  - Common control recommendations for each

- Firefighter / Emergency Access
  - 1-2 reasons for FF Use
  - Key differences vs. ECC access:
    - Audit of reason and transactions used
    - Emergency vs. routine use
  - 2-3 FF best practices

Assignment Questions

- What is "function modules" in last week lecture?
- Who within an organization should have Centralized Emergency Access (CEA)?
- How can we audit an automated process in SAP?
- Where do business function play in SAP security – risk remediation and access request process?
- From a typical business' perspective, how often are policies reviewed/revised?

Break Time

Risk / Control Matrix
Final Exercise

Risk / Control Matrix: Design Approach

Risks

Define

Control Objectives

Drive

Control Activities / Controls

Influence

Control, system and Security Design + Implementation

- Automated Controls
- Manual Controls
- Application Security
- Segregation of Duties
- Approvals
- Reports
- Procedures

CONTROL DESIGN

Risk / Control Matrix: Final Exercise

- Agenda
  - Prior Class *(April 4)*: Part 1 - Identify Risks
  - Last Class *(April 11)*: Part 2, 3
    - Risk Priority (Severity & Likelihood)
    - Identify Controls
    - Link Controls to Risks

  - *Today*: Part 4 - Complete Control Definitions
  - *April 25*: Part 5, 6 - Control Process / Audit Details; Personal Questions
  - *Due April 28 11:59 PM:* Assignment Submission

Risk / Control Matrix: Final Exercise

Part 4: Augment key controls information for the Order to Cash (OTC) process at GBI

- Tab: Part 2 – GBI Controls
- Control Description (Columns F -> K) Mark each using taxonomy provided
  - Control Owner (Title): Choose **one** title from Appendix 1 or define appropriate missing title
- Financial Statement Assertions (Columns L-> Q) Mark with **X**
- Control Risk Assessment (Columns R -> U) Taxonomy column top
- Financial Statement Impact (Columns V -> AK) Mark statements impacted with **x**

Extra Slides

Risk / Control Matrix: Final Exercise

Part 1:

a) Analyze the key risks that exist for the Order to Cash (OTC) process at GBI

b) Define and document the key risks that exist for the Order to Cash (OTC) process at GBI

- Tab: Part 1 – GBI Risks
- Identify at minimum 25 risks in the process
- Identify a minimum 4 risks in each of the OTC sub-processes:
  - ✓ **OR&H**: Order Receipt and Handling
  - ✓ **MF**: Material Flow (shipping)
  - ✓ **CI**: Customer Invoicing
  - ✓ **PR&H**: Payment Receipt and Handling

Risk Assessment

Risk / Control Matrix: Final Exercise

Part 2: Identify key controls for the Order to Cash (OTC) process at GBI

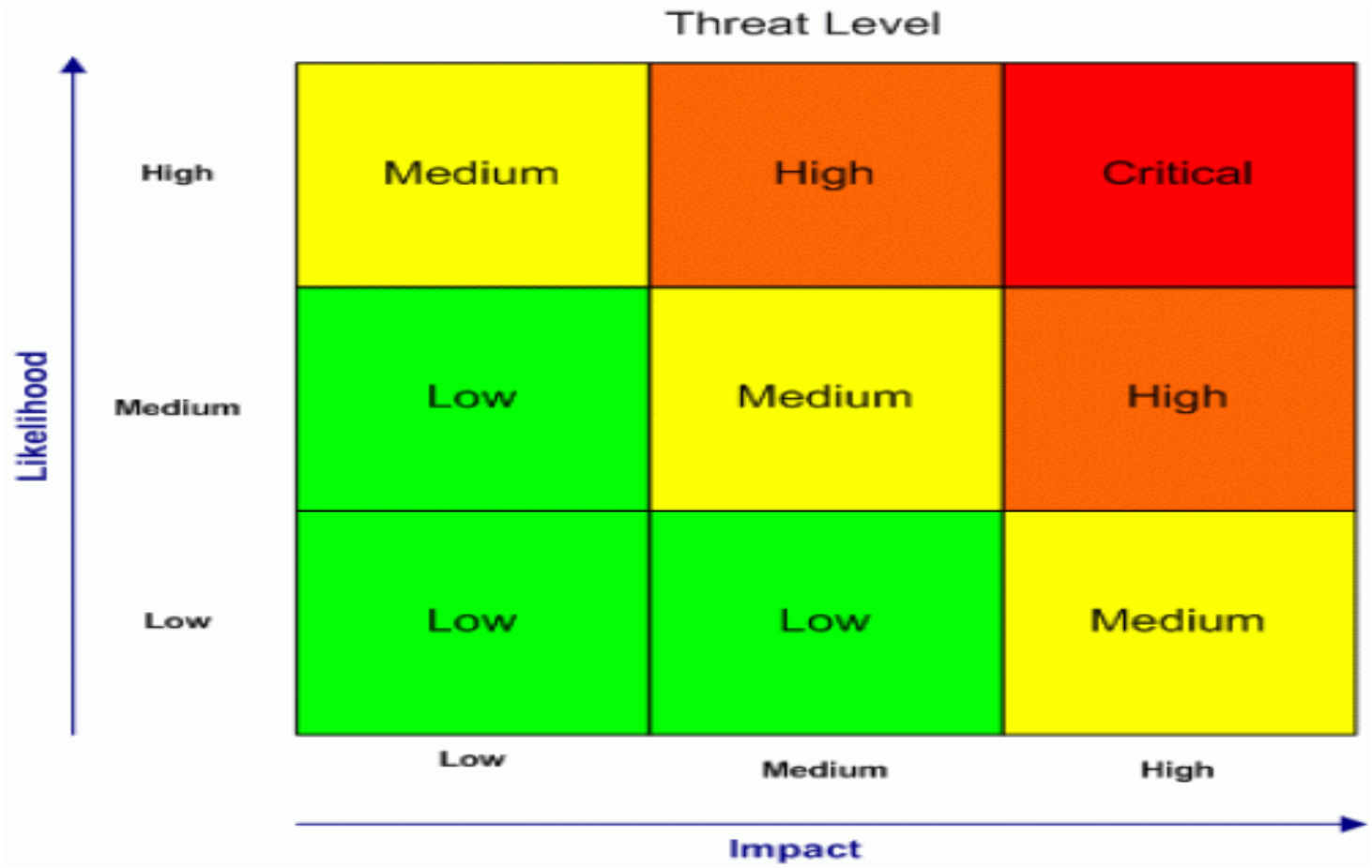
- Tab: Part 2 – GBI Controls
- Identify at minimum 15 controls for the process
- Identify a minimum 3 controls in each of the OTC sub-processes:
  - ✓ **OR&H**: Order Receipt and Handling
  - ✓ **MF**: Material Flow (shipping)
  - ✓ **CI**: Customer Invoicing
  - ✓ **PR&H**: Payment Receipt and Handling
- At least two (2) controls must be Automated / Config controls

Risk / Control Matrix: Final Exercise

Part 3: Link Risks (Part 1) to the Controls (Part 2)

- Tab: Part 1 – GBI Risks
- At least one (1) control must be identified for each risk identified as High Severity or High Likelihood / Frequency
- A given control may address multiple risks (listed once in Part 2 tab and multiple times in Part 1 tab)
- A given risk may be addressed by multiple controls (listed once in Part 1 tab and multiple times in Part 2 tab)
- Risks without out a control:
  - ✧ Acceptable Risk: Business agrees no controls will be developed
  - ✧ TBD (To Be Determined)

Extra Slides



SAP System Characteristics

Integrated Database

- All transactions stored in one common database in thousands of tables
- Module automatically create entries in other modules (e.g. OTC creates financial postings)
- Auditors need to understand the flow of information
- Databases can be accessed by any module
- Users view the system as Transactions, documents and reports
- SAP modules are transparent to users

Risk / Control Matrix: Final Exercise

Parts

1. Analyze and define the key risks that exist for the Order to Cash (OTC) process at GBI
2. Guided by the risks you identified (esp. the High Severity and High Likelihood / Frequency risks) identify the key controls that will be used in the OTC process.
3. Link the Risks from Part 1 to the controls in Part 2.
4. Complete definition of the controls (classifications, links to assertions, etc.)
5. Write auditable control process documentation for 1 manual and 1 automated (configuration) control identified.
6. (Individual vs. Team submission): Couple questions about your work as a team to complete this and other exercises. (Optional)
   Details will be announced via a blog post in last couple weeks of class.

Risk / Control Matrix: Design Approach

Risks

Define

Control Objectives

Drive

Control Activities / Controls

Influence

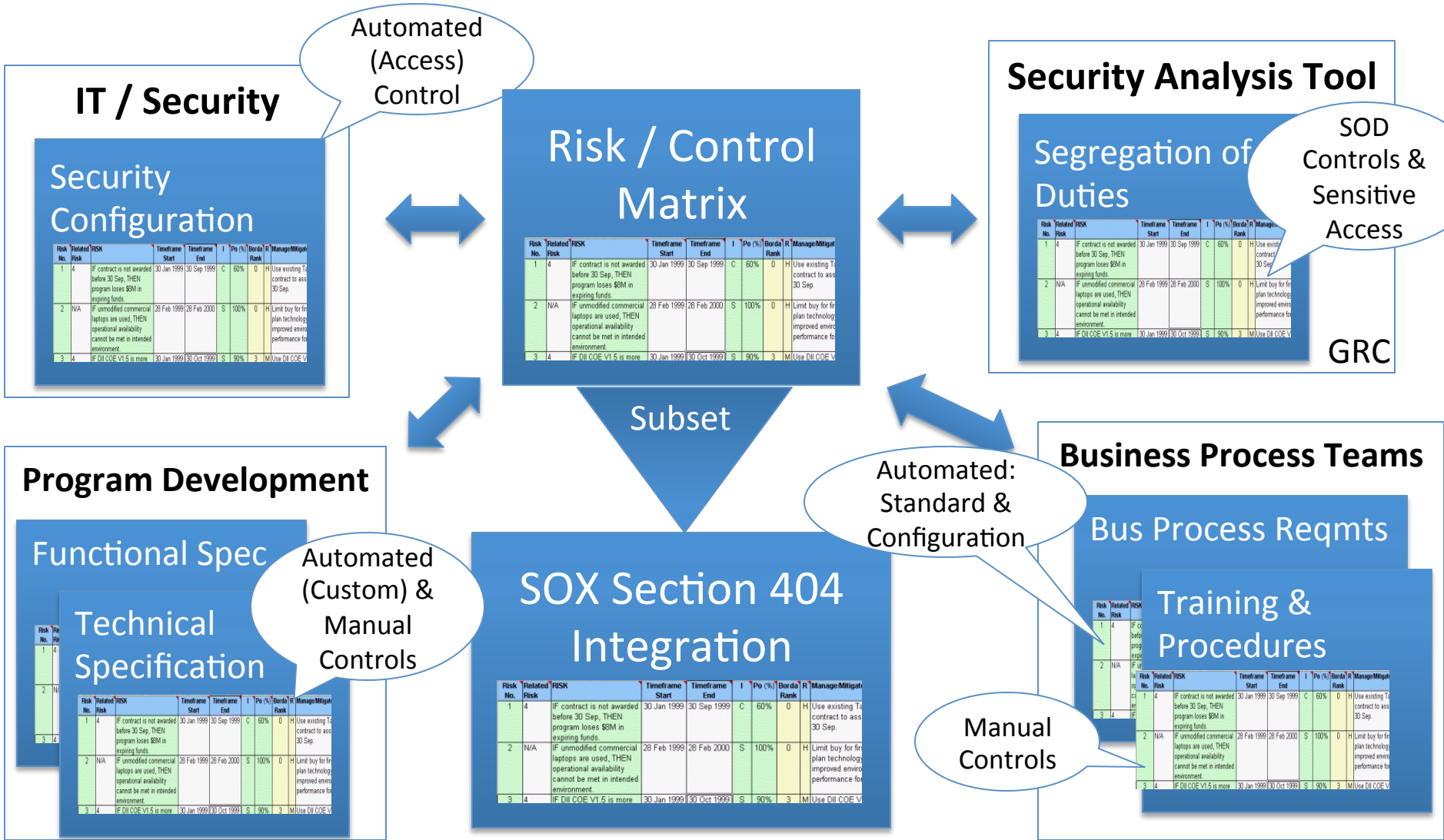
Control, system and Security Design + Implementation

- Automated Controls
- Manual Controls
- Application Security
- Segregation of Duties
- Approvals
- Reports
- Procedures

CONTROL DESIGN

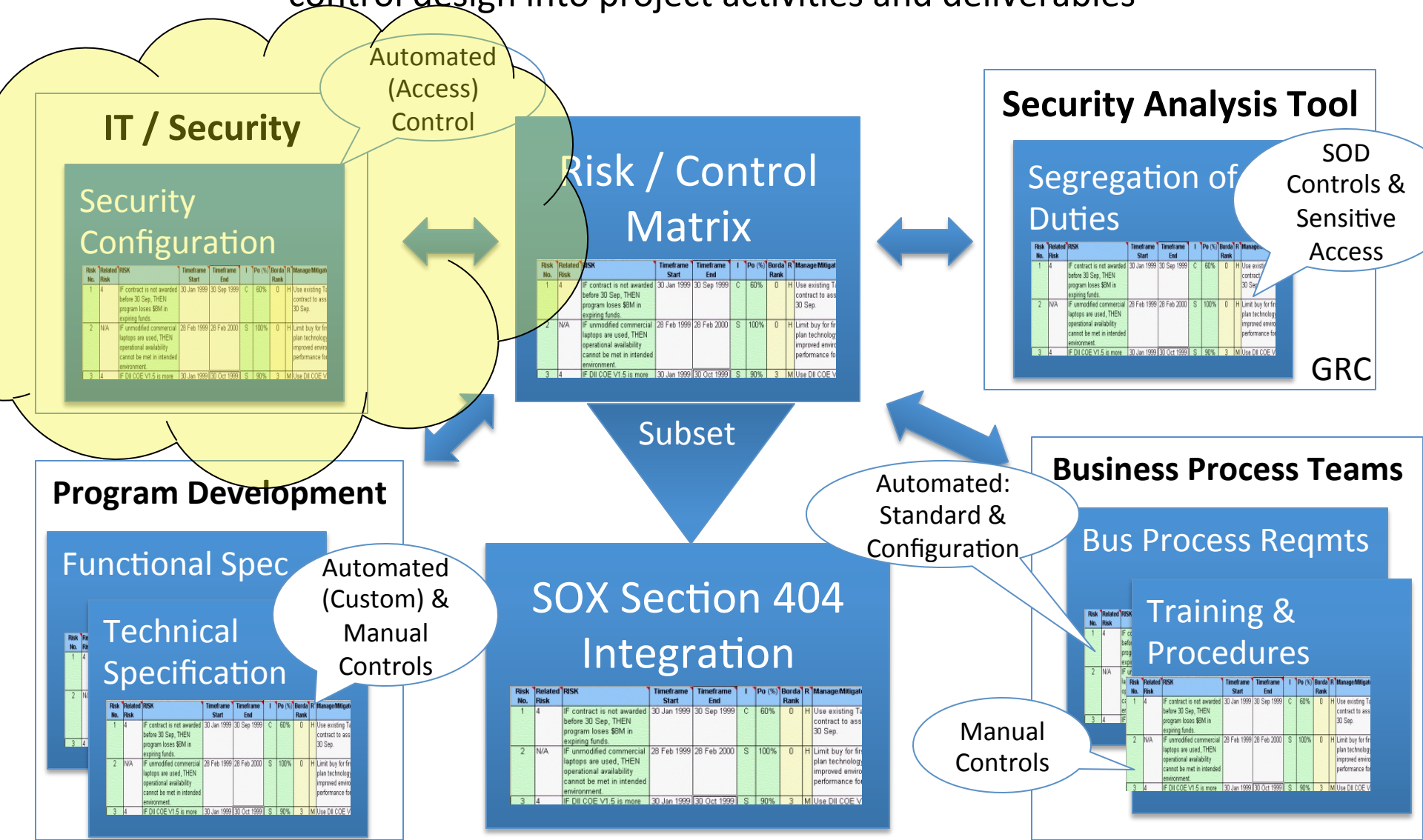
Controls: Integration Points

Risk/Control Matrix can serve as the primary vehicle for integrating control design into project activities and deliverables



Controls: Integration Points

Risk/Control Matrix can serve as the primary vehicle for integrating control design into project activities and deliverables



Firefighter