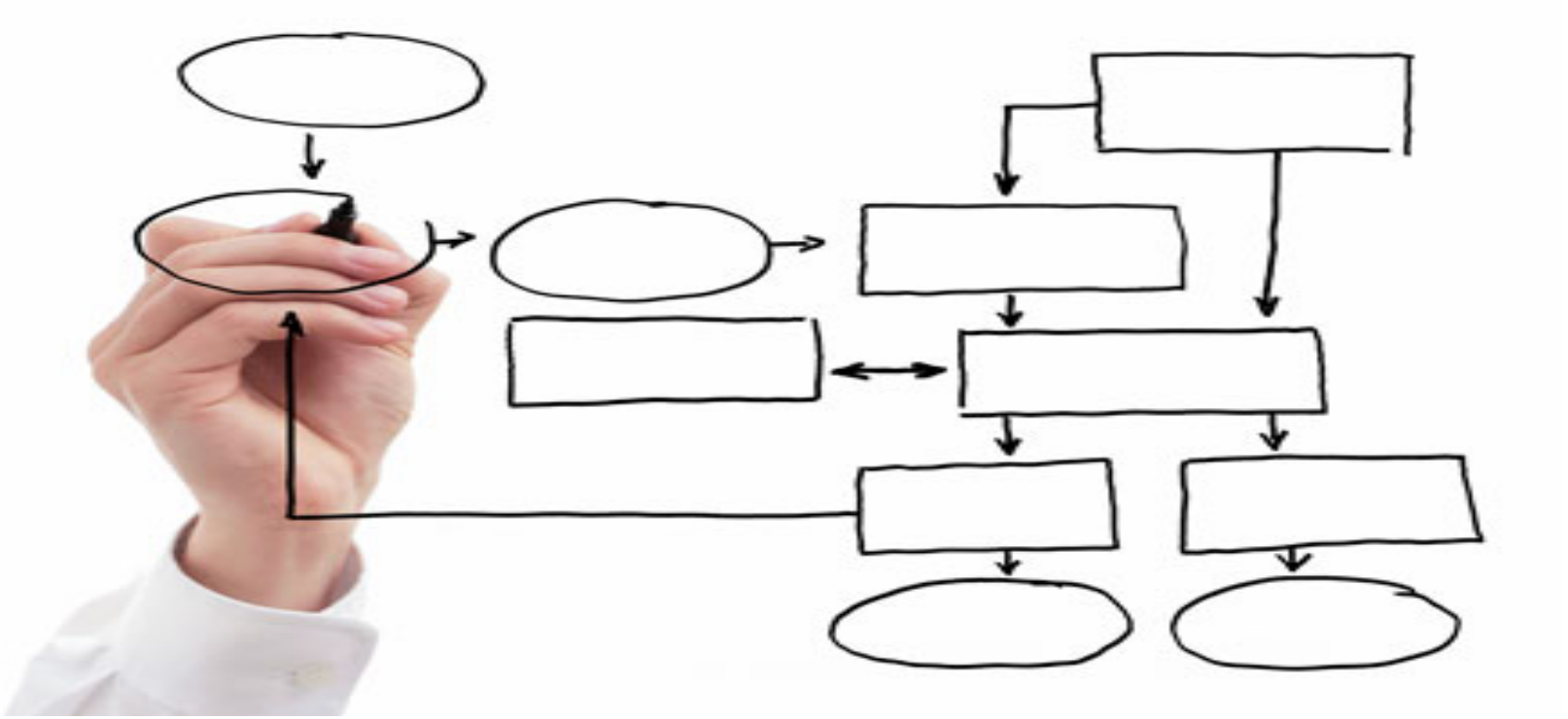


MIS 5121: Business Processes, ERP Systems & Controls

Week 12: *Table Security, Systems Development 2, Control Framework*

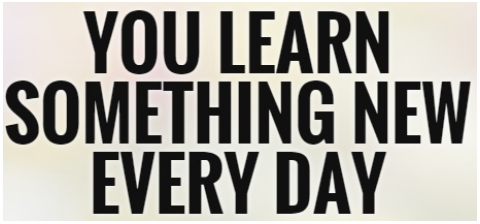
FOX | MIS
Management Information Systems

Edward Beaver
Edward.Beaver@temple.edu
ff

Video: Record the Class

Discussion

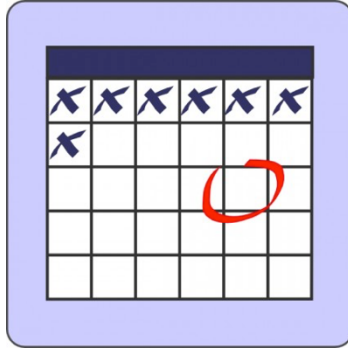
- Something really new, different you learned in this course in last week



- Questions you have about this week's content (readings, videos, links, …)?

- Question still in your mind, something not adequately answered in prior readings or classes?

MIS 5121: Upcoming Events



- Guest Moderator?: Auditor's Perspective - *Week 12??*
- Guest Moderator?: SAP Futures - Week 13??

- Last Hybrid class (on-line, Alter Hall 602): *December 12*
- Final Exercise (Risk Control Matrix)-*Due: December 15*

2016 F

Auditing: Helping Hands

Kapish Vanvaria

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

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

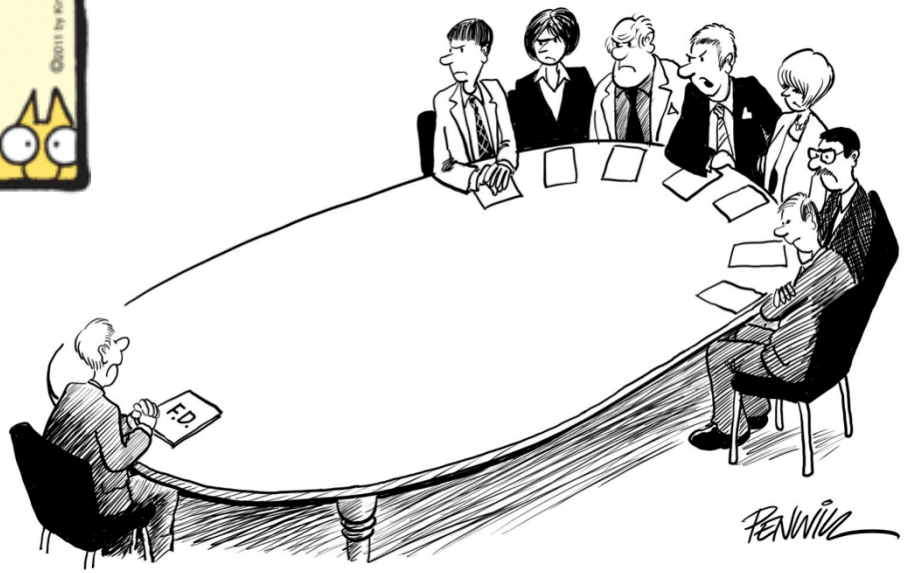
- Have you personally detected a fraud scenario in your audit? If so, please explain
- How do you maintain your independence? Is that easy?
- What are the general methodologies used for auditing?
- How do you classify risks?
- Since SAP can be customized in so many ways, how does an auditor know what to audit when everything is different with each client?
- 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 : Auditor's Topics 2015

- What are the general methodologies used for auditing?
- How do you classify risks?
- How do you review Segregation of Duties (modules vs. employees)?
- Since SAP can be customized in so many ways, how does an auditor know what to audit when everything is different with each client?

Success with Internal and External Auditing
My Personal Experience

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



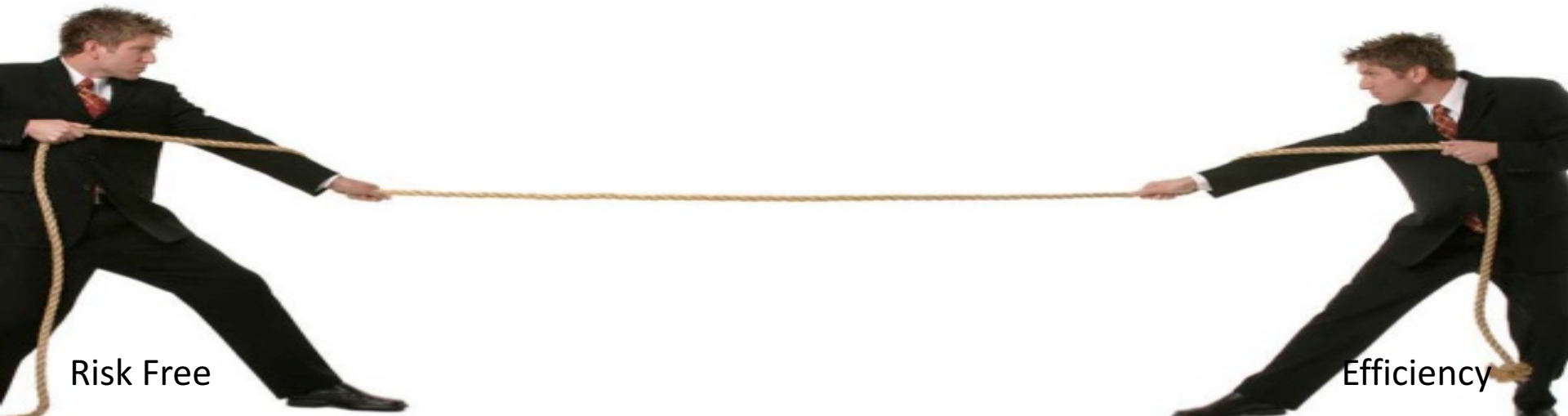
"WE DON'T WANT YOU TO VIEW THIS AUDIT COMMITTEE AS BEING IN ANY WAY CONFRONTATIONAL"

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



Risk / Control Matrix: Design Approach

Risks

Define

Control Objectives

Drive

Control Activities / Controls

Influence

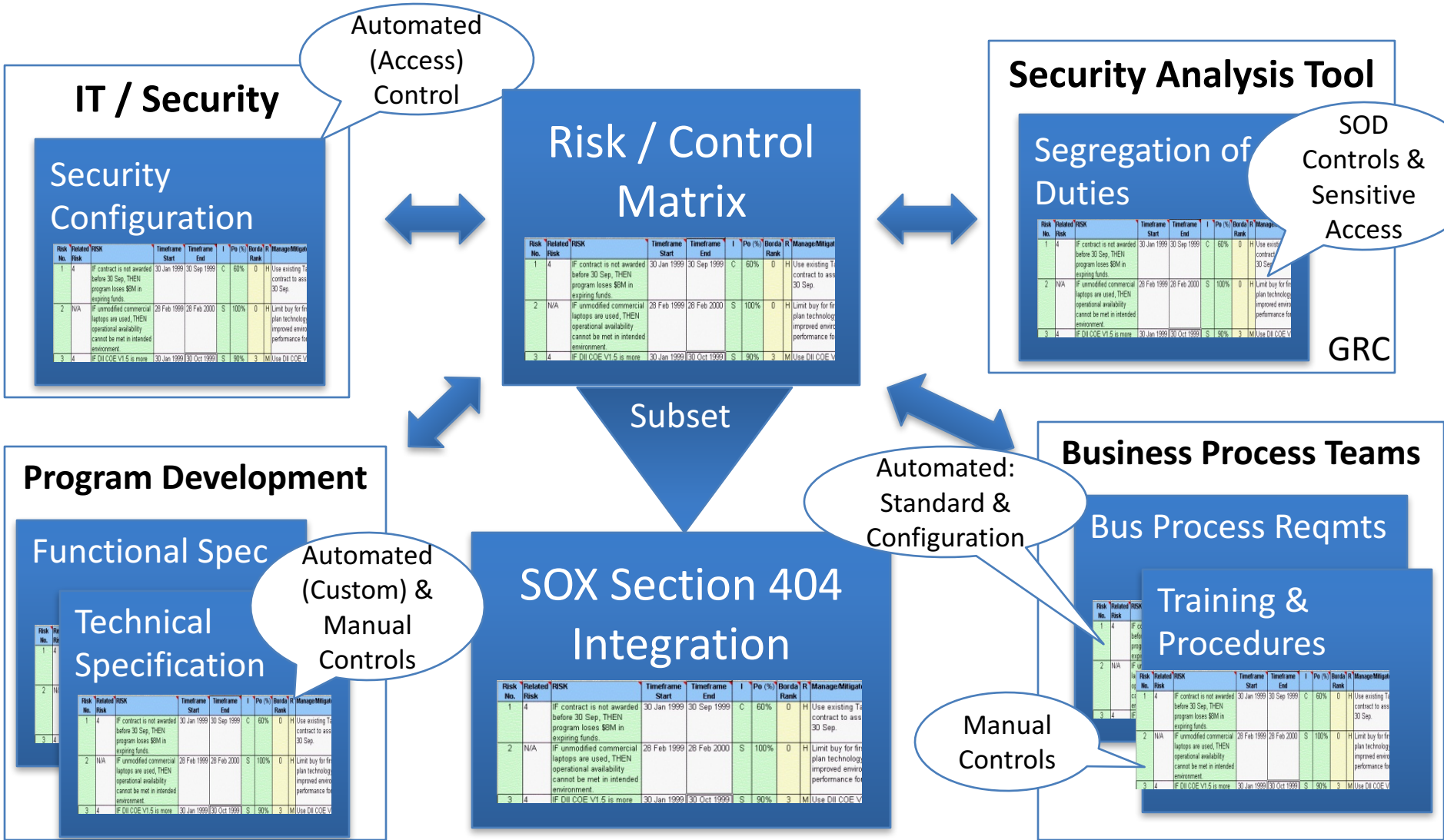
Control, system and Security Design + Implementation

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

CONTROL DESIGN

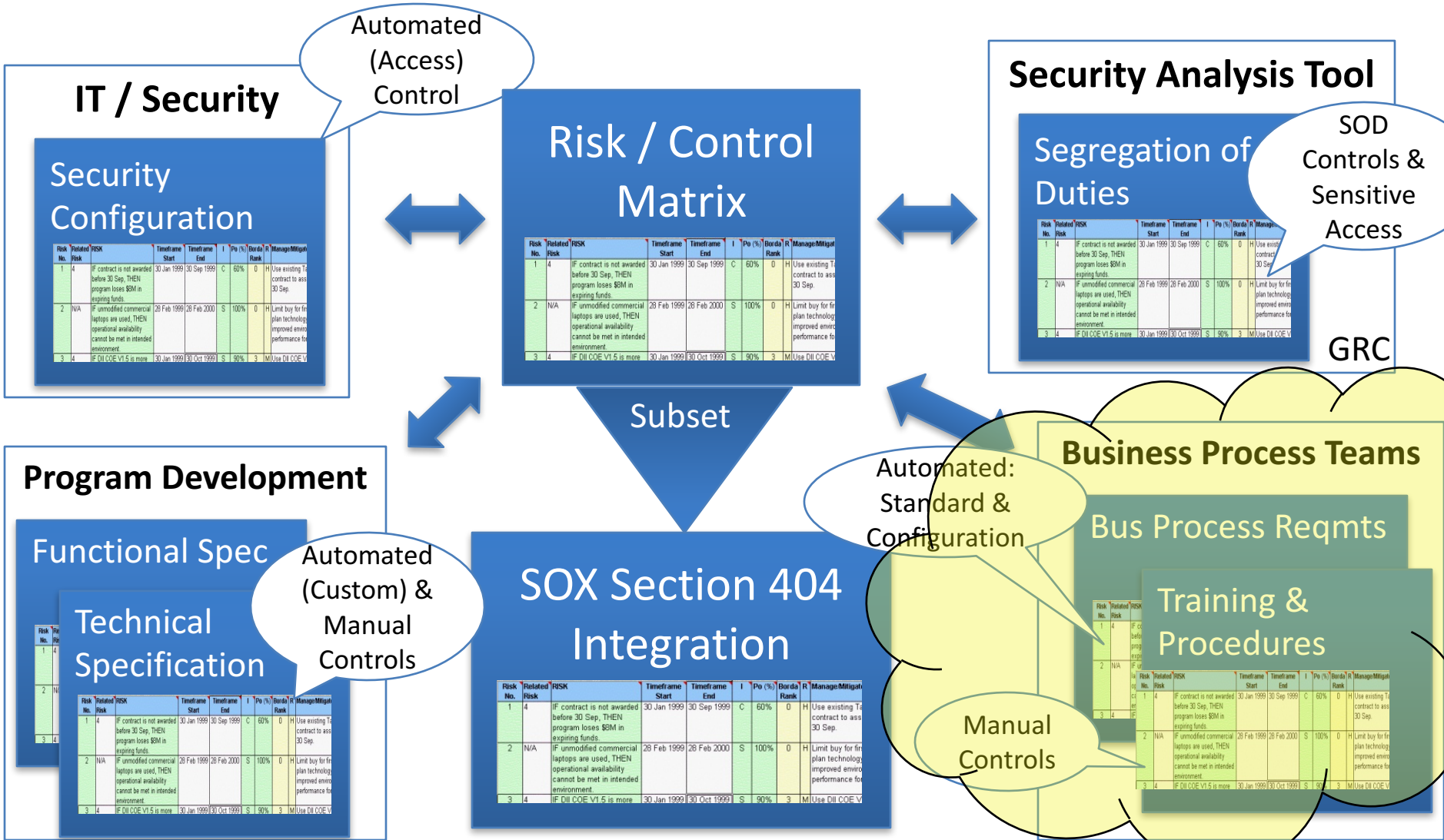
Controls: Integration Points

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



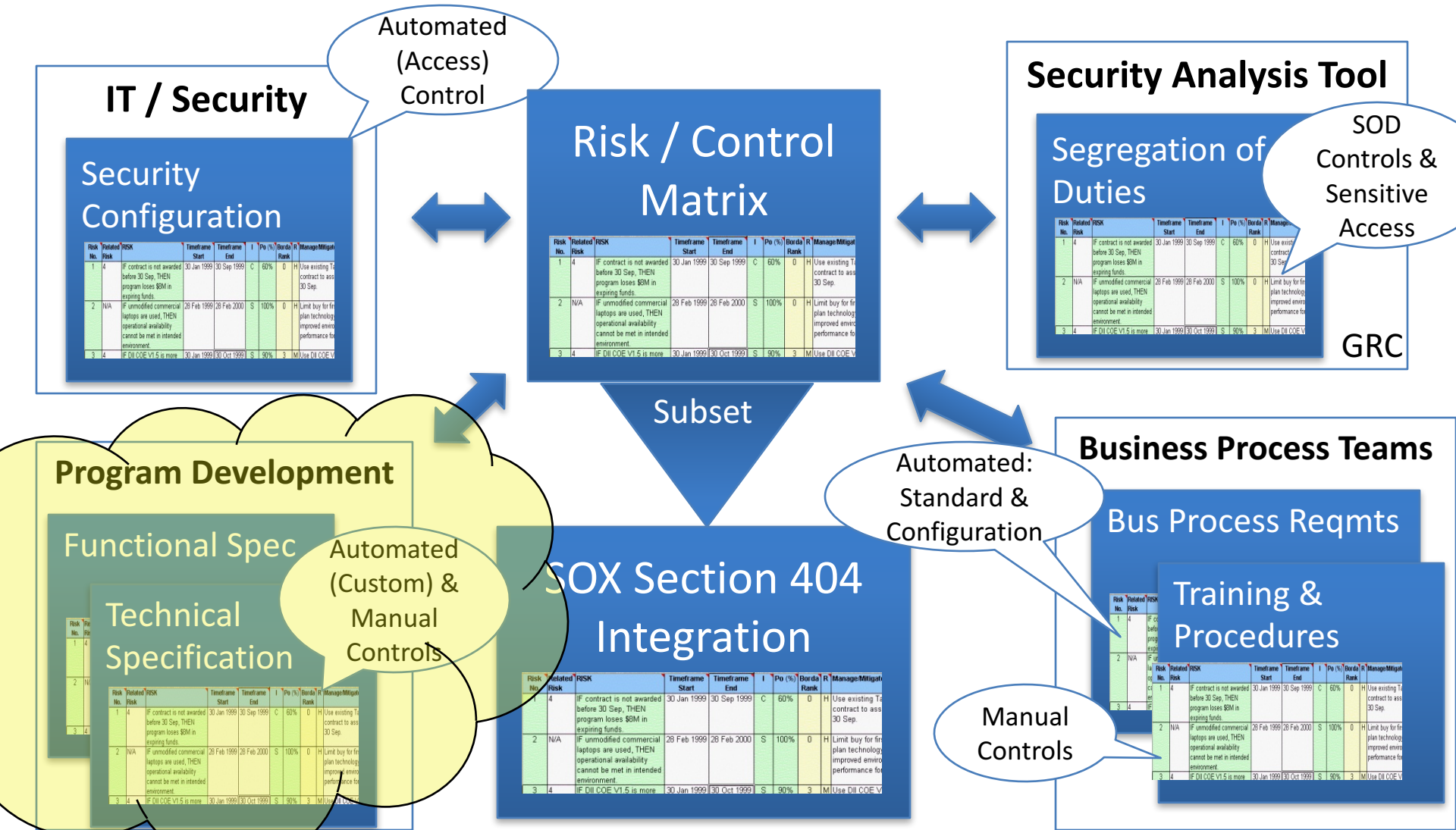
SAP: Table Driven System Execution

- SAP Processing is customized using thousands of **Configuration tables**
  - Access via the 'Implementation Guide' (Transaction SPRO)
  - Entries determine how transactions are processed
  - Entries also support implementation of controls (e.g. processing parameters and limits)

- ERP Systems are Dynamic
  - Configuration table values and therefore system processing, are continually changed (process changes, business structure, etc.
  - Effective processing and control Requires:
    - Managed Design
    - Documentation

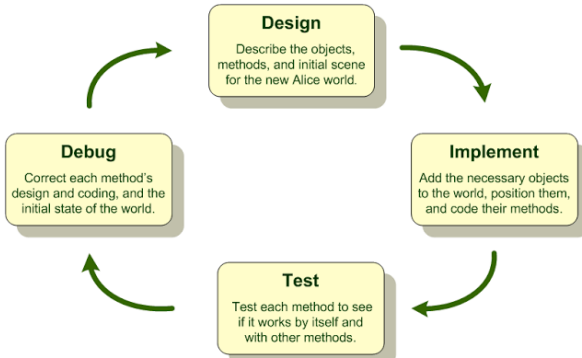
Controls: Integration Points

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

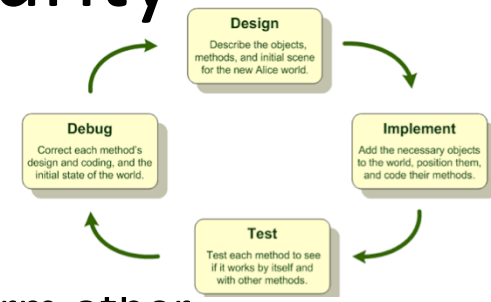


Program & Development Security

- Types of Development Objects (FRICE)
  - **F**orms – outputs (invoices, Purchase orders, ...)
  - **R**eports – custom reports
  - **I**nterfaces – SAP to other systems
  - **C**onversions – Data migration
  - **E**nhancements – Change system logic, use additional fields, etc.
    - User-Exits: defined SAP branches to custom code (lower risk)
    - Change SAP code (high risk, long term extra maintenance)
  - Workflow – non-config components, logic
- Development: custom programs
  - Typically ABAP (SAP SQL extension programming language)

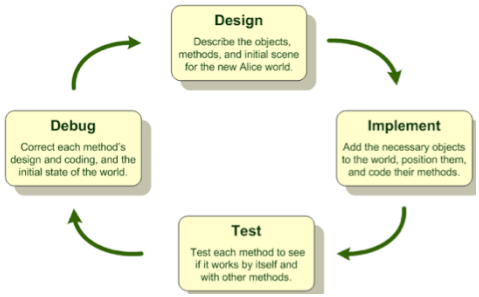


Program & Development Security



- Is program code 'good'
  - Does what it's supposed to do
  - Limited to requirements only (not branch off to perform other nefarious actions)
  - Well-behaved: doesn't mess up other programs, logic, operation of ERP system
- Good Development Practices
  - Clear, documented, approved requirements defined before coding
  - Define Requirements, Design Logic before major coding (e.g. use of function modules for common logic)
  - Peer Code Reviews
  - Experienced development leadership
  - Test, Test, retest **BEFORE** moving to PRD (strong change management governance)

Risk and *Recommendation*
Program Security



Risks:

- Unintended, nefarious uses of program code
- Users capable of executing programs directly can compromise standard controls (access security, audit trails)
- Users with access to run ALL programs are allowed to run all executable programs (note not all programs are executed directly)
- Display access to ABAP code gives backdoor access to program execution
- Debug authority provides unsecured table viewing and table change

Recommendations:

- Active review, manage program code deails
- Access to run programs restricted via SAP Security / Authorizations
- Further secure programs via assignment to authorization groups
- Basis Admin no Display access to ABAP code (prevent backdoor access)
- Debug authority restricted to effectively monitored ‘emergency users’

Breakout Activity – Rules

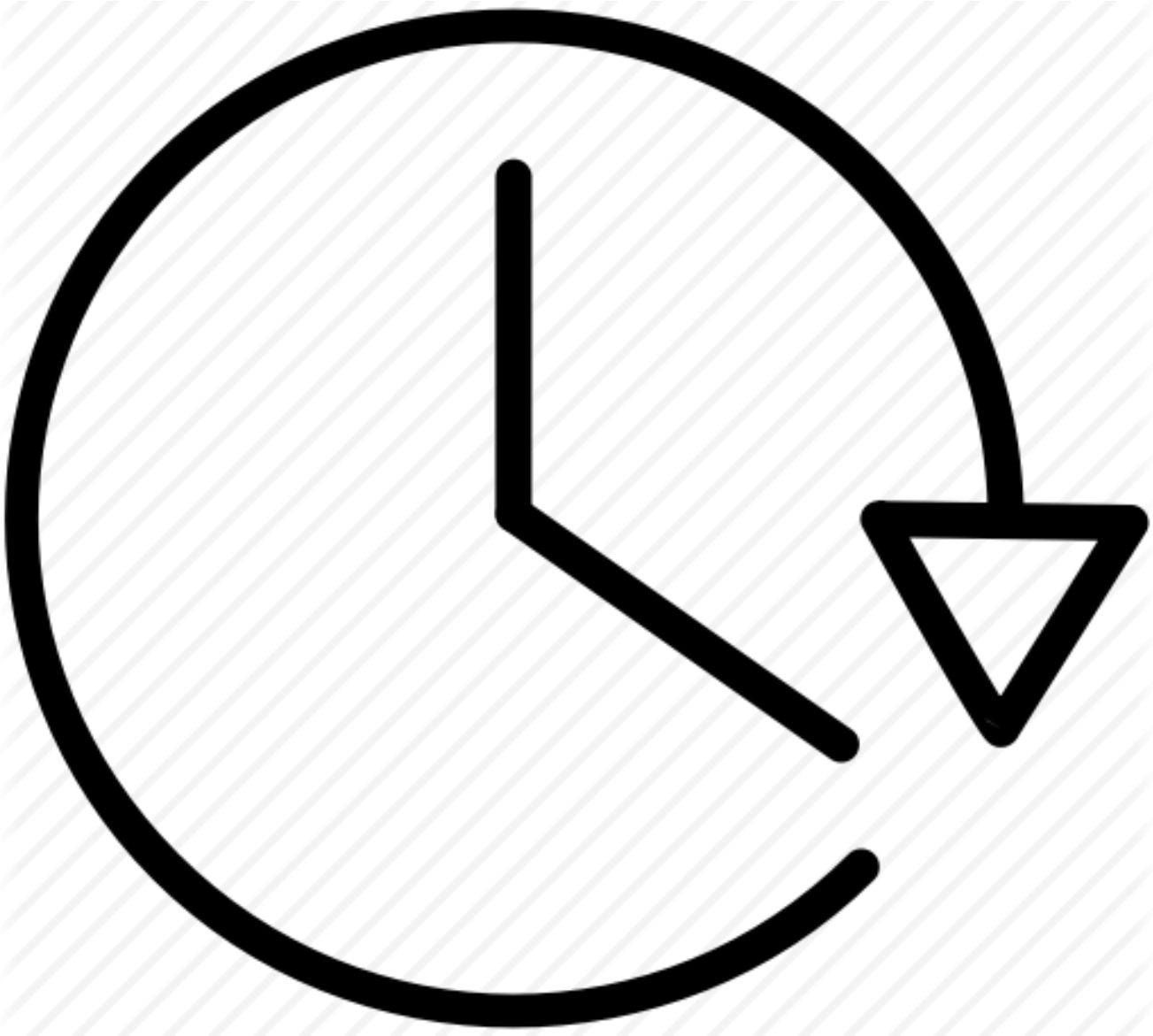
- Break into teams – max of 5 people / team
  - Diversity a must.
- Assignment – return via WebEx Notes or Word Document
- How: WebEx breakout?
- Time: assigned today 20 min (including break)
  - Start back **on-time**

Breakout Question

Suppose you are a perspective customer or partner of SAP. Given what you know about businesses processes, ERP systems and related controls:

What questions would you ask SAP?

- _____
- _____
- _____



Report Back

Risk / Control Matrix
Final Exercise

GLOBAL BIKE INC.

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
  - Last Class *(November 14)*: Part 1 (Identify Risks)
  - **This Class *(November 28)*: Part 2, 3**
    - Risk Priority (Severity & Likelihood)
    - Identify Controls,
    - Link Controls to Risks
  - Future Class *(December 5)*: Part 4 (Complete Control Definitions)
  - Future Class *(December 12)*: Part 5, 6 (Control Process / Audit Details; Personal Questions)
  - *Due December 15 11:59 PM:* Assignment Submission

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

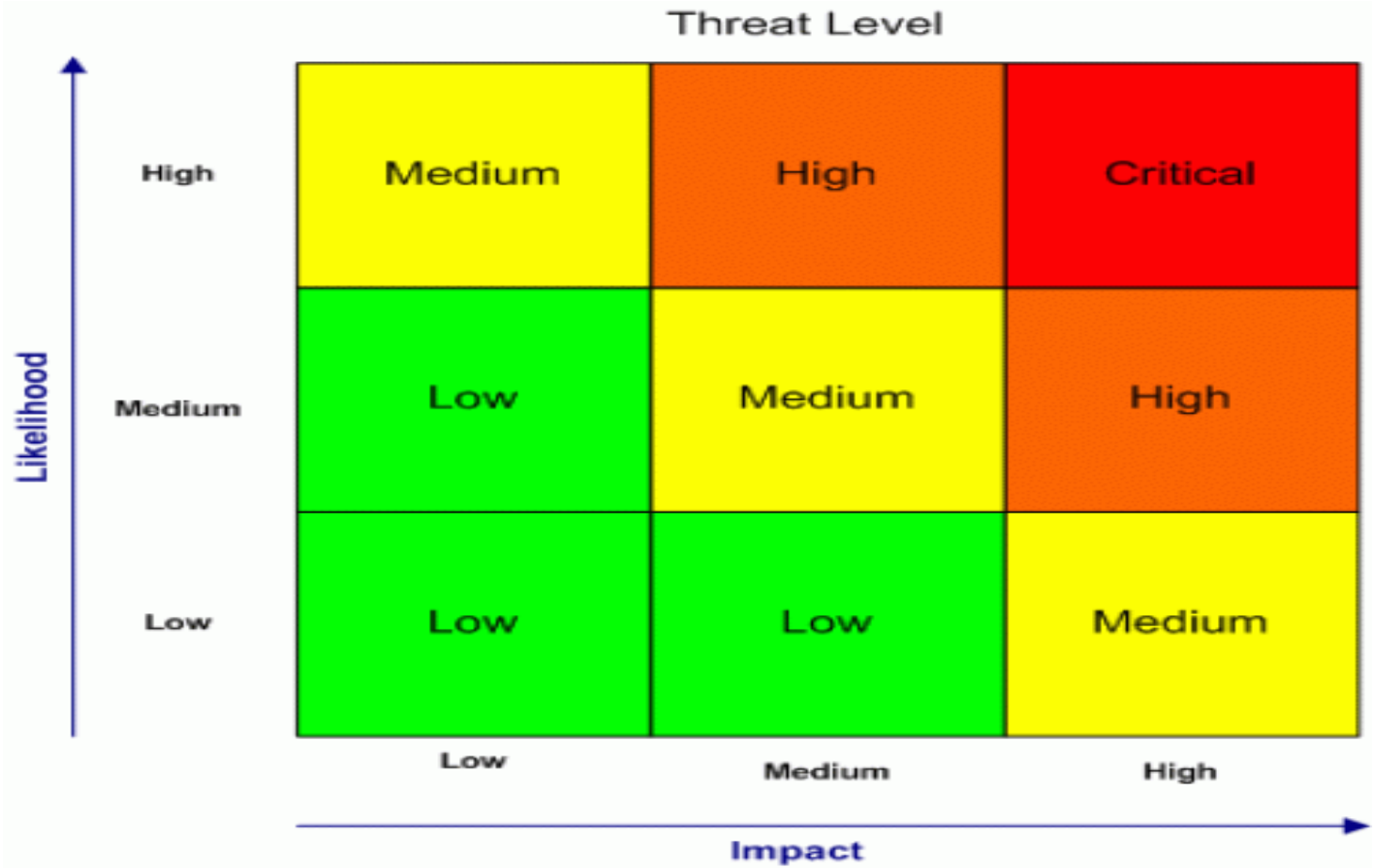
Risk / Control Matrix: Final Exercise

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

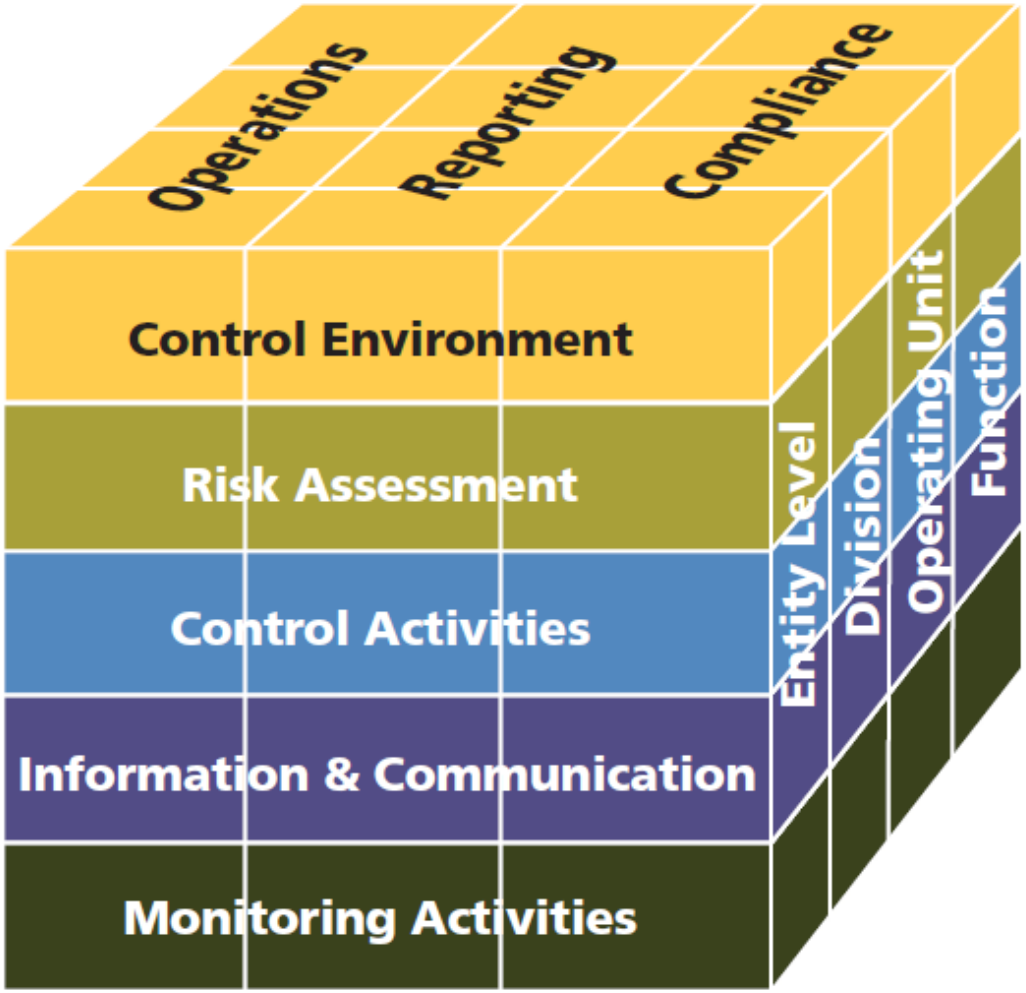
- Tab: Part 1 – GBI Risks
- At least one (1) control must be identified for each risk identified as High Severity or High Likelihood / Frequency
- A given control may address multiple risks (listed once in Part 2 tab and multiple times in Part 1 tab)
- A given risk may be addressed by multiple controls (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

Extra Slides



COSO Framework (2013)



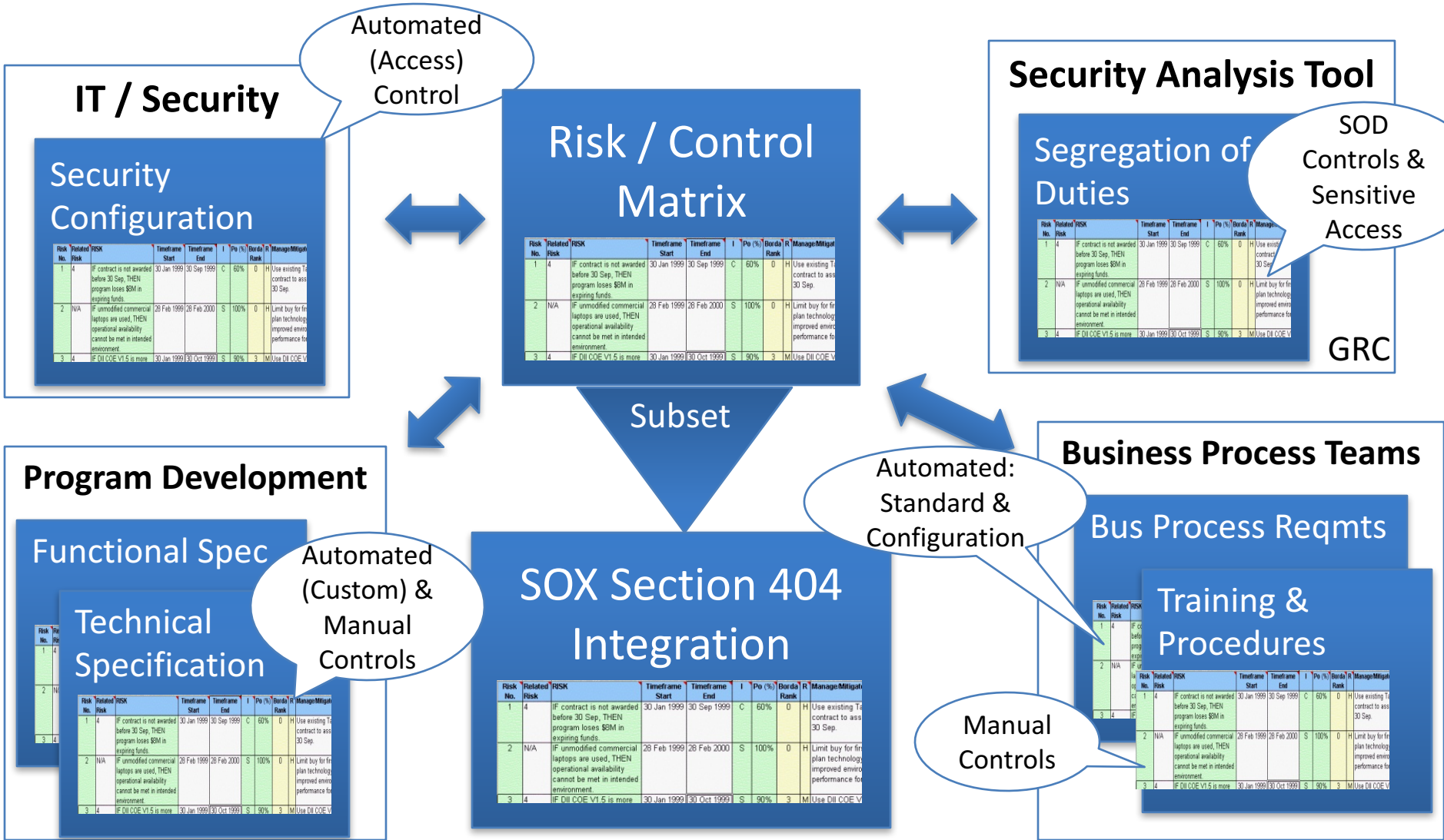
COSO Framework (2013)

Codification of 17 principles embedded in the original Framework

Control Environment	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
Risk Assessment	6. Specifies relevant objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change
Control Activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys through policies and procedures
Information & Communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring Activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

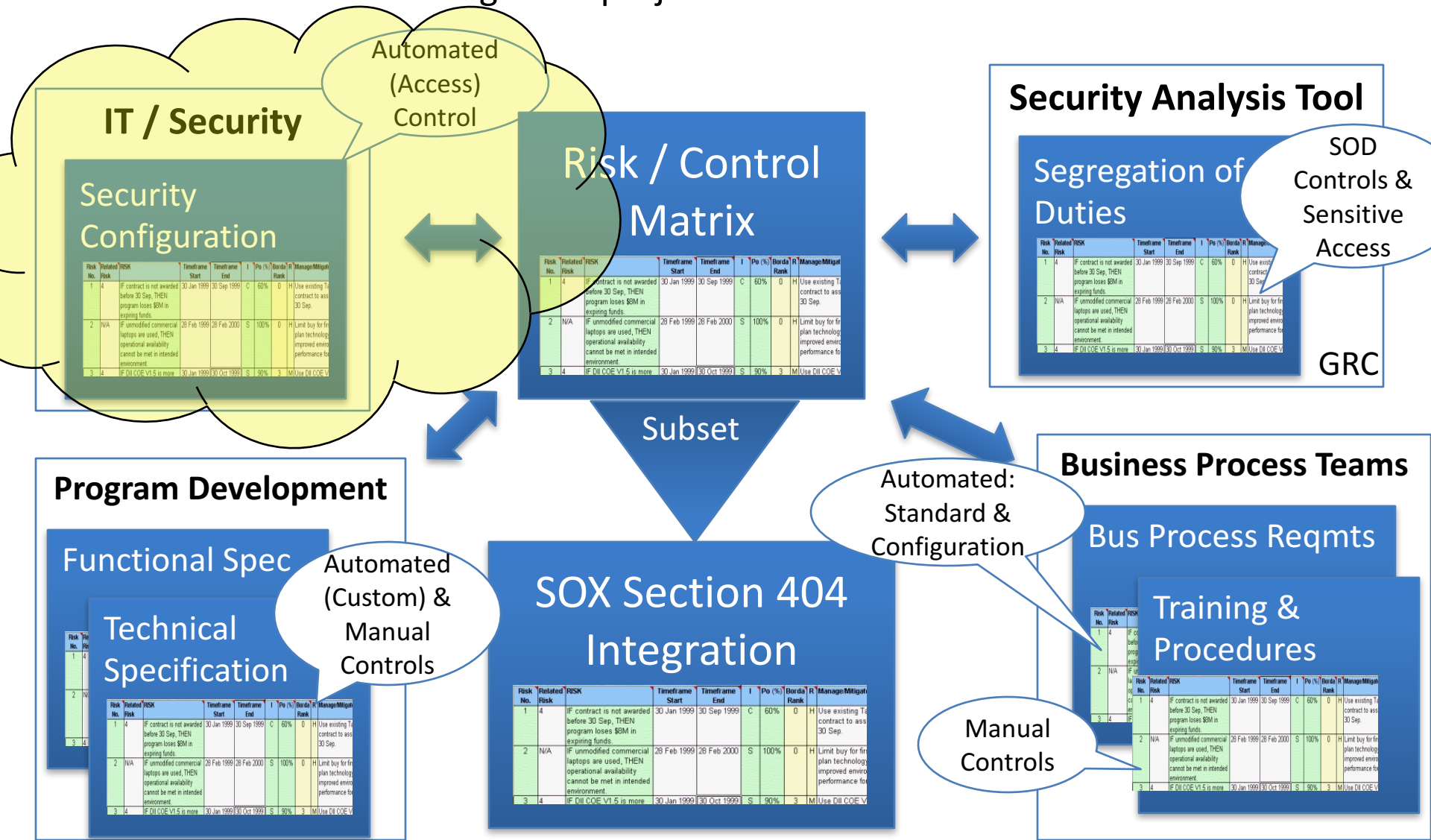
Controls: Integration Points

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



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.