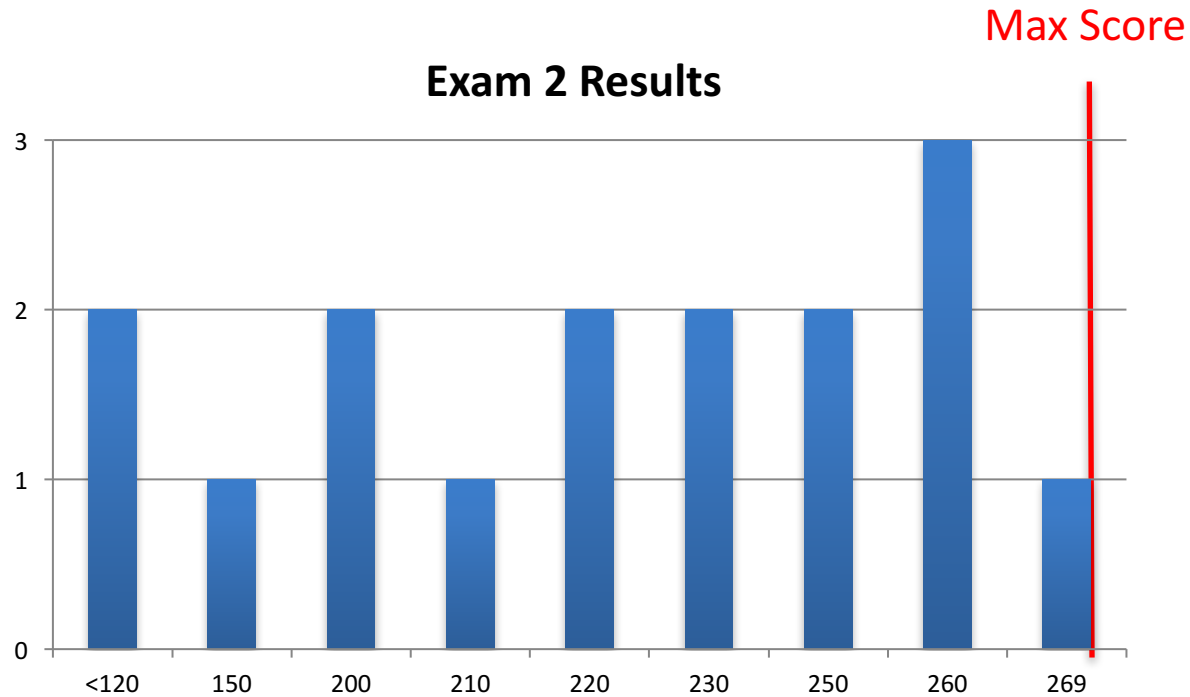


MIS 5121: Business Processes, ERP Systems & Controls
Week 12: *Auditing, Systems Development 2,
Table Security, Control Framework*

Video: Record the Class



Exam 2 Test Results

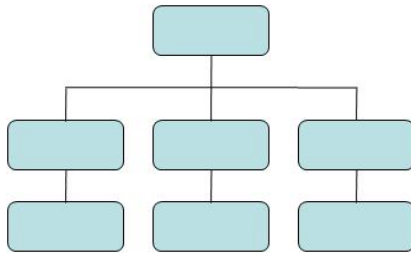


- No 'curve' because one student achieved max score
- If you have questions on how I graded, your response, etc. send me an email
- Weeks 1-10 course content that may be on Final Exam in next slides

Business Function vs. Process

Function

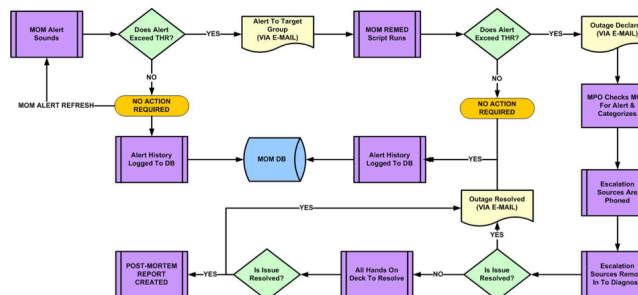
‘An operation / group who perform related tasks routinely to achieve a part of an organization’s mission .’



Business Dictionary

Process

‘A series of logically related activities / tasks performed together to produce a defined set of results.’

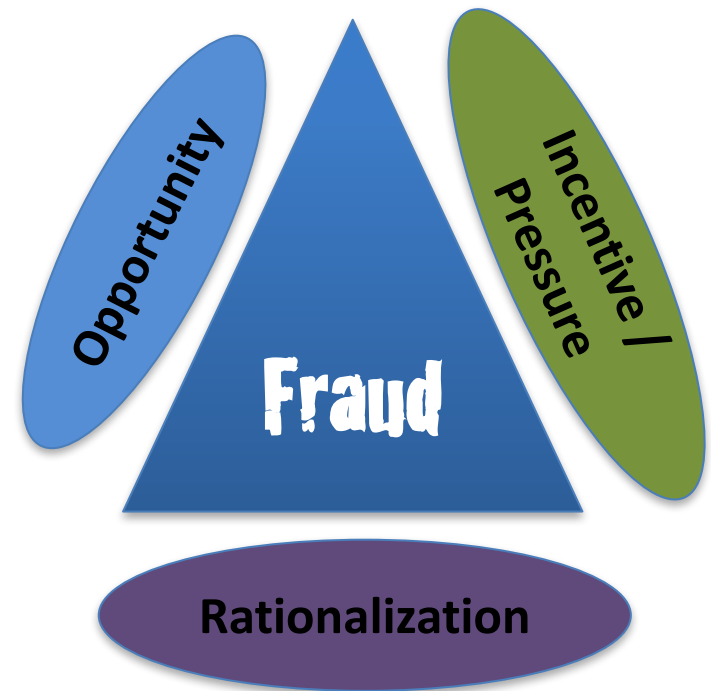


Business Dictionary

Environment Favorable to Fraud

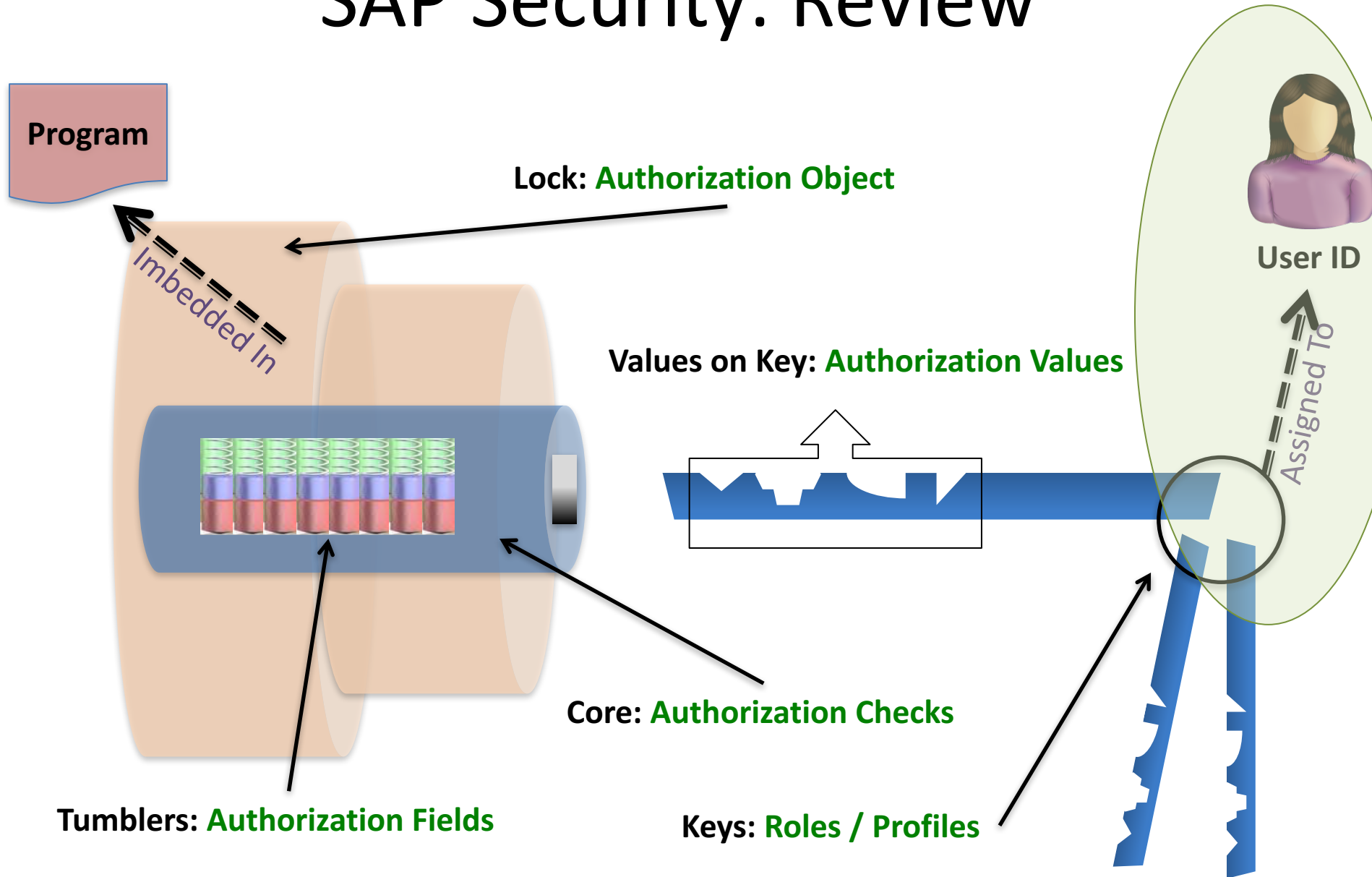
Framework for spotting high-risk situations

- Perceived **opportunity** (*I can do it / conceal it and not get caught*)
 - Poor internal controls
 - Lack of oversight
- **Incentive or Pressure** (*Financial or emotional force pushing to commit fraud*)
 - Meet expectations
 - Avoid criticism
 - Cover a mistake
 - Personal failures, needs
- **Rationalization** (*Personal justification for dishonest actions*)
 - Low compensation
 - Company is profitable

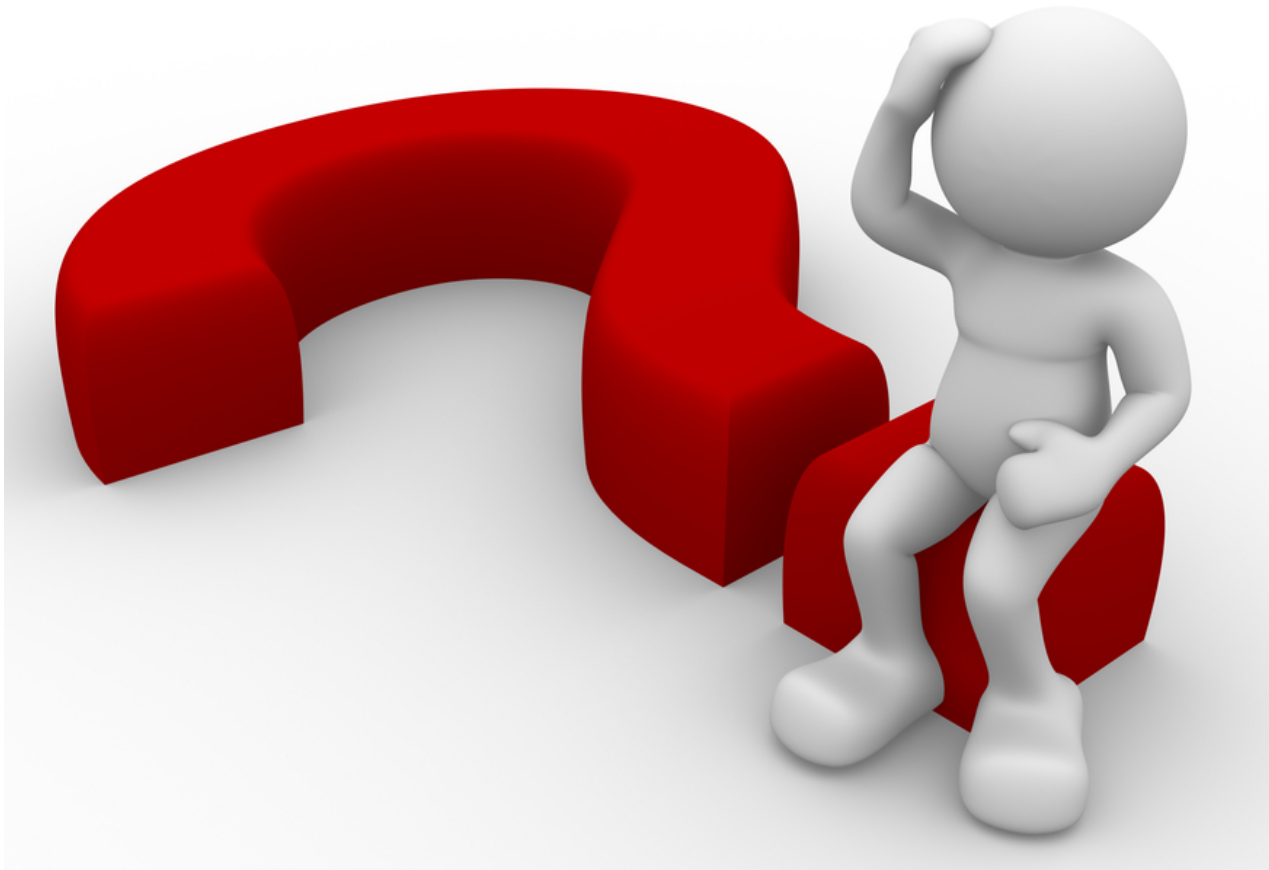


Fraud Triangle

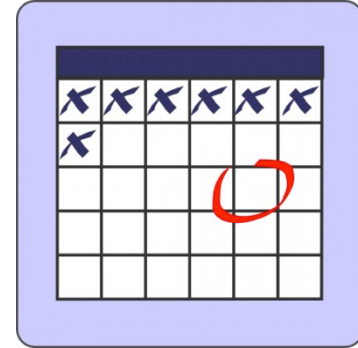
SAP Security: Review



Questions Re: Exam 2



MIS 5121: Upcoming Events



- December 11: ITACS Advisory Council Social Event – 5:00 till 6:00
 - You are invited, encouraged to attend
 - Class will start at 6:00
- Final Exercise (Risk Control Matrix)-*Due: Dec 14*
- Final Exam: *December 18 (at class time)*



Discussion

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

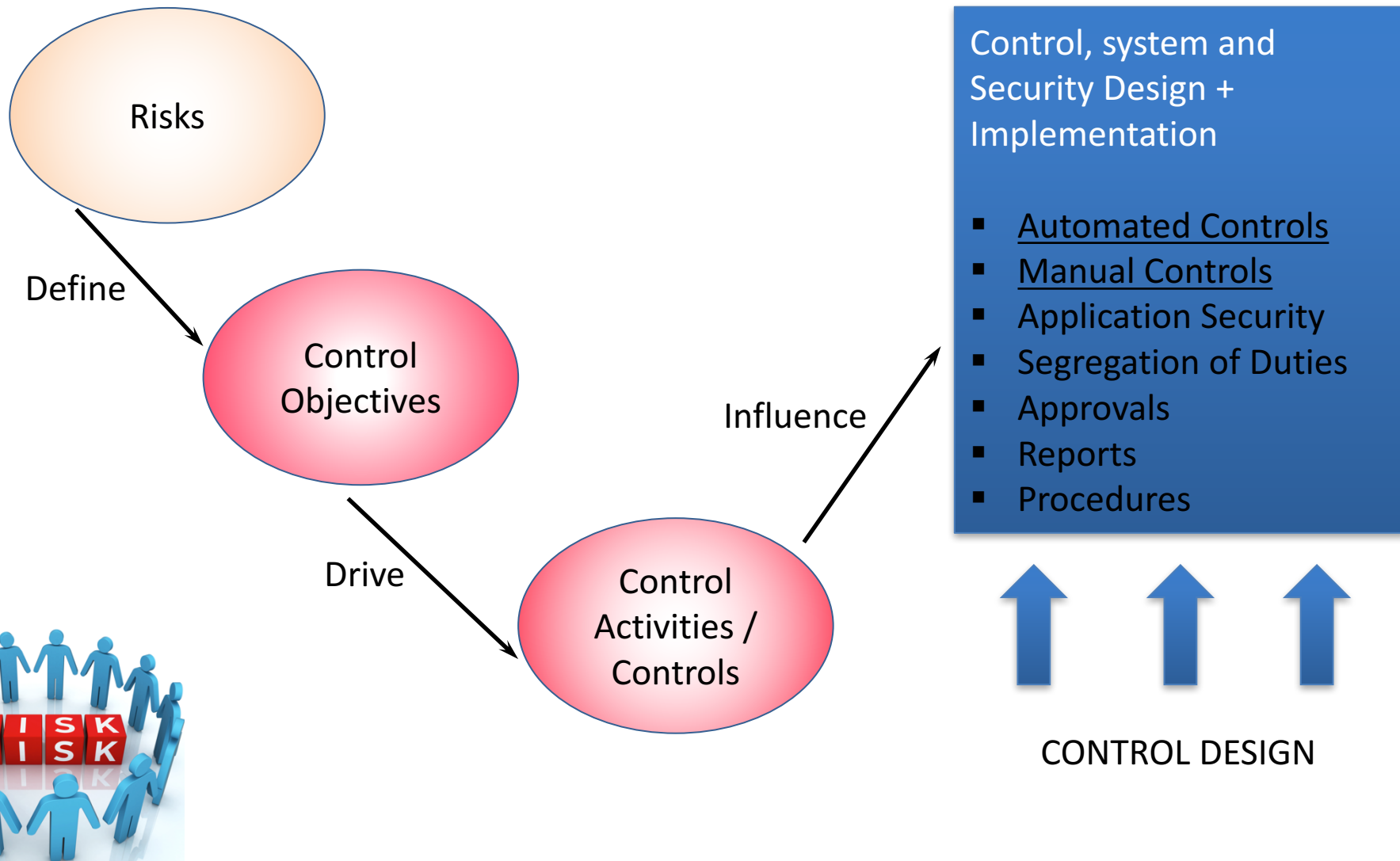
**YOU LEARN
SOMETHING NEW
EVERY DAY**

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



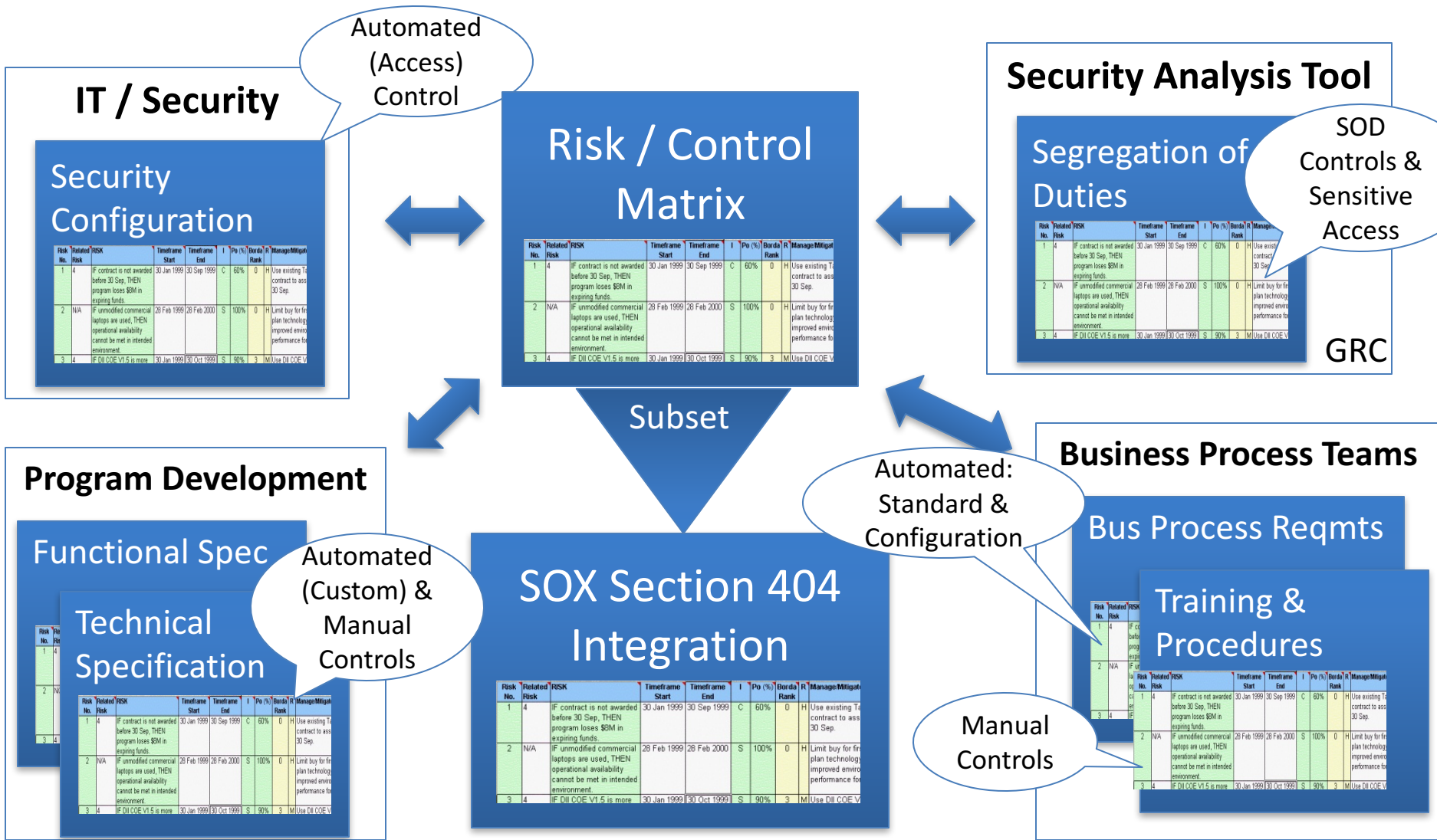
❖ Question still in your mind, something not adequately answered in prior readings or classes?

Risk / Control Matrix: Design Approach



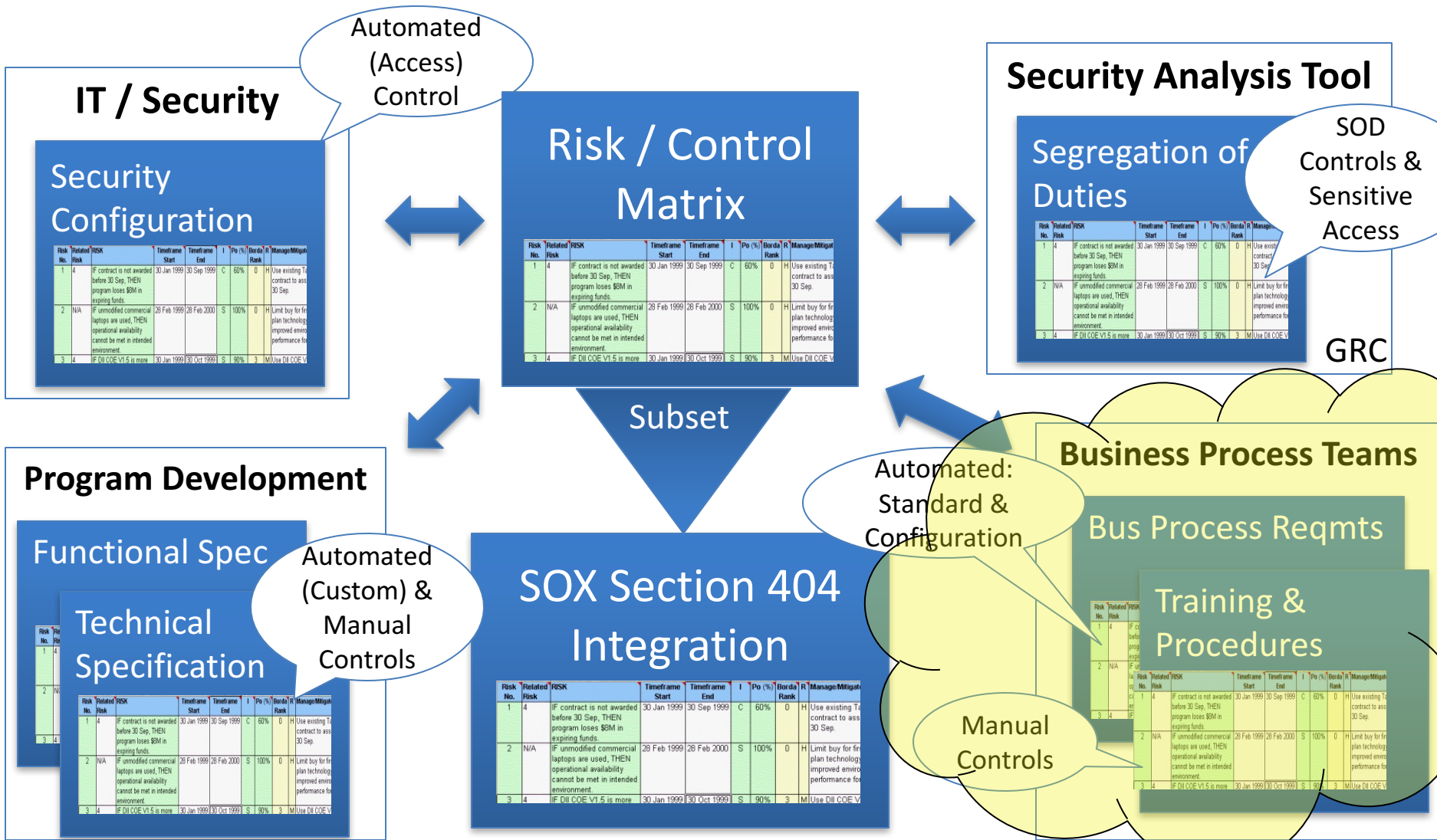
Controls: Integration Points

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



Real World Control Example

Configuration Control (Order to Cash)



Control Definition Outline

- **Reference #:** OCRW-608
- **Control Activity:** Tolerance groups have been appropriately configured inline with managements intentions.
- **Process** Order to Cash
- **Sub-Process** Cash Application
- **Location** Headquarters
- **Frequency:** **Used:** Z: Multiple x/day
Review: A: Annual
- **Automated: vs. Manual:** Automated
- **Control type:** P: Preventative

Control Owner:

Order to Cash Business
Process Architect



Configuration Review Procedure

- Transaction: SPRO (SAP Reference IMG)
 - Financial Accounting (New) > Accounts Receivable and Accounts Payable > Business transactions > Open item clearing > Clearing Differences > Define Tolerances for Customers/Vendors
- Click on Company Codes under review
- Ensure tolerance settings are appropriate

- Conclusion: _____



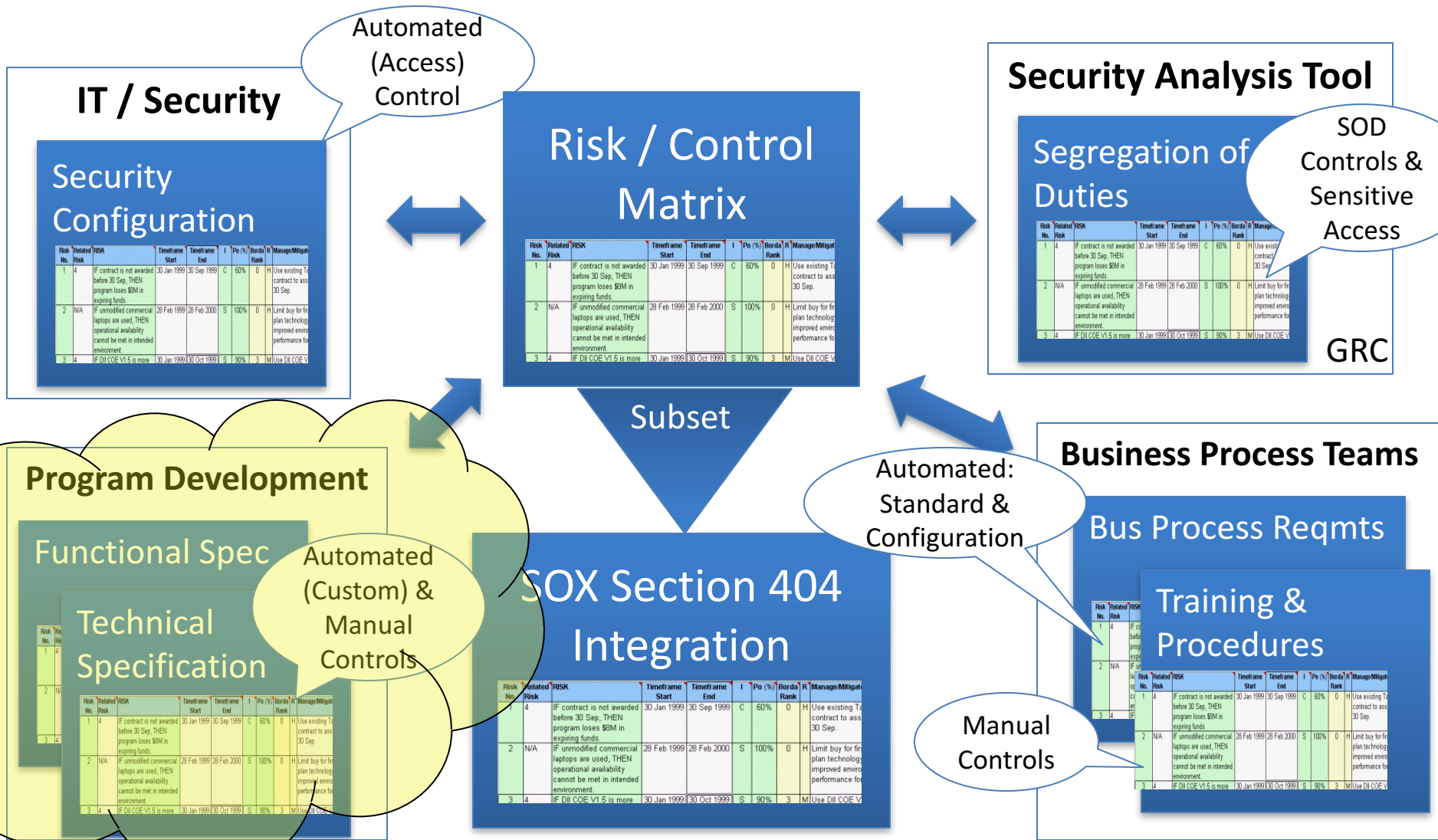
Configuration Review Procedure (Alternate)

- Download related configuration table.
Transaction: SE16N
 - Table: T043G (Tolerances for Groups of Customers /Vendors)
- Download table
- Review active entries and ensure tolerance settings are appropriate
- Conclusion: _____



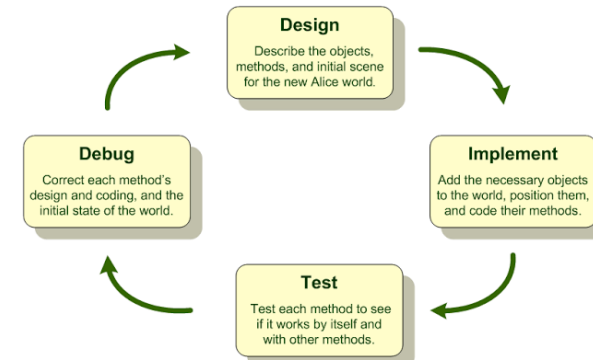
Controls: Integration Points

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



Program & Development Security

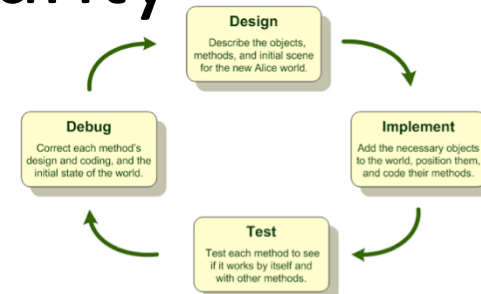
- Types of Development Objects (FRICE)
 - ✧ Forms – outputs (invoices, Purchase orders, ...)
 - ✧ Reports – custom reports
 - ✧ Interfaces – SAP to other systems
 - ✧ Conversions – Data migration
 - ✧ Enhancements – Change system logic, use additional fields, etc.
 - User-Exits: defined SAP branches 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'

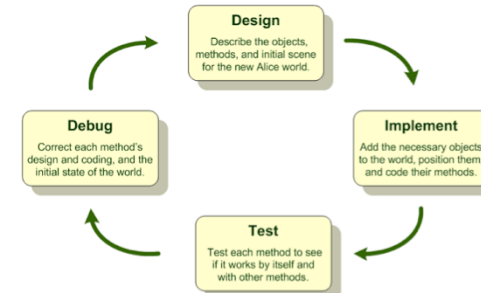
- ✧ Does what it's supposed to do
- ✧ Limited to requirements only (not branch off to perform other nefarious actions)
- ✧ Well-behaved: doesn't mess up other programs, logic, operation of ERP system



➤ 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:

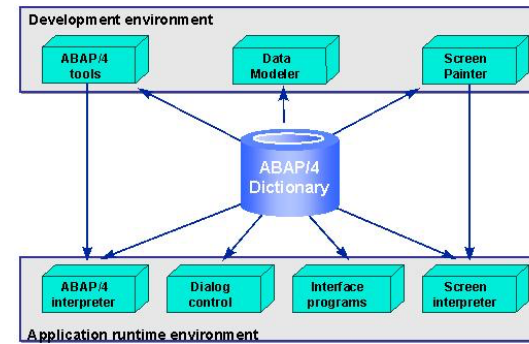
- Unintended, nefarious uses of program code
- Users capable of executing programs directly can compromise standard controls (access security, audit trails)
- Users with access to run ALL programs are allowed to run all executable programs (note not all programs are executed directly)
- Display access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

Recommendations:

- Active review, manage program code details
- 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'

Risk and Recommendation

Data Dictionary



Risks:

- PRD Access to S_DEVELOP Allows direct changes to Data Dictionary which could compromise integrity of the data
- Any Data Dictionary change could compromise integrity of the data

Recommendations:

- No one (including Basis Administrators) should have update access to Data Dictionary in Production (PRD)
- Changes to data dictionary performed in DEV, tested in QA and migrated to PRD per change management process
- Developer access restricted appropriately using SAP Security / authorization concept



Key IT Controls Overview

- Program, Development, Data Dictionary
 - 2-3 risks that exist
 - Common control recommendations for each



Risk and Recommendation

Change Documents

Risks:

If users are not restricted from maintaining change documents, the system audit trail from changes documents could be deleted accidentally or via malicious intent



Recommendations:

Users in production have activity level of security object S_SCD0 set to '08' (Display Change Documents).

Investigate ways access to maintenance of change documents could be further restricted (locking transaction)

Risk and Recommendation

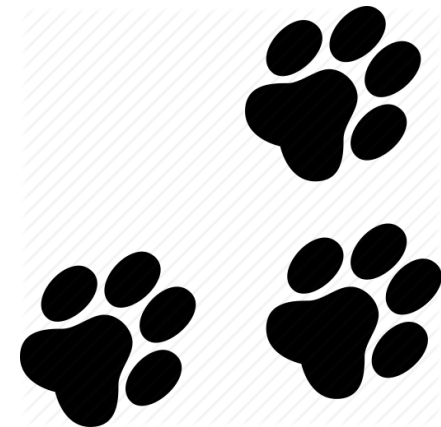
System Logs and Trace Files

Risks:

- If audit files (Logs and traces) are not secured at the operating system level for each application server, they could be maliciously deleted

Recommendations:

- Secure folders where log and traces files are stored at the operating system level
- Develop and use procedures for how to review and run traces at part of routine system security monitoring



Key IT Controls Overview

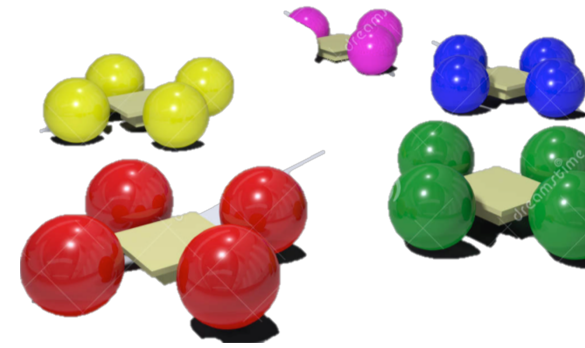
- Logs and Traces

- 2-3 risks that exist

- Common control recommendations for each



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**

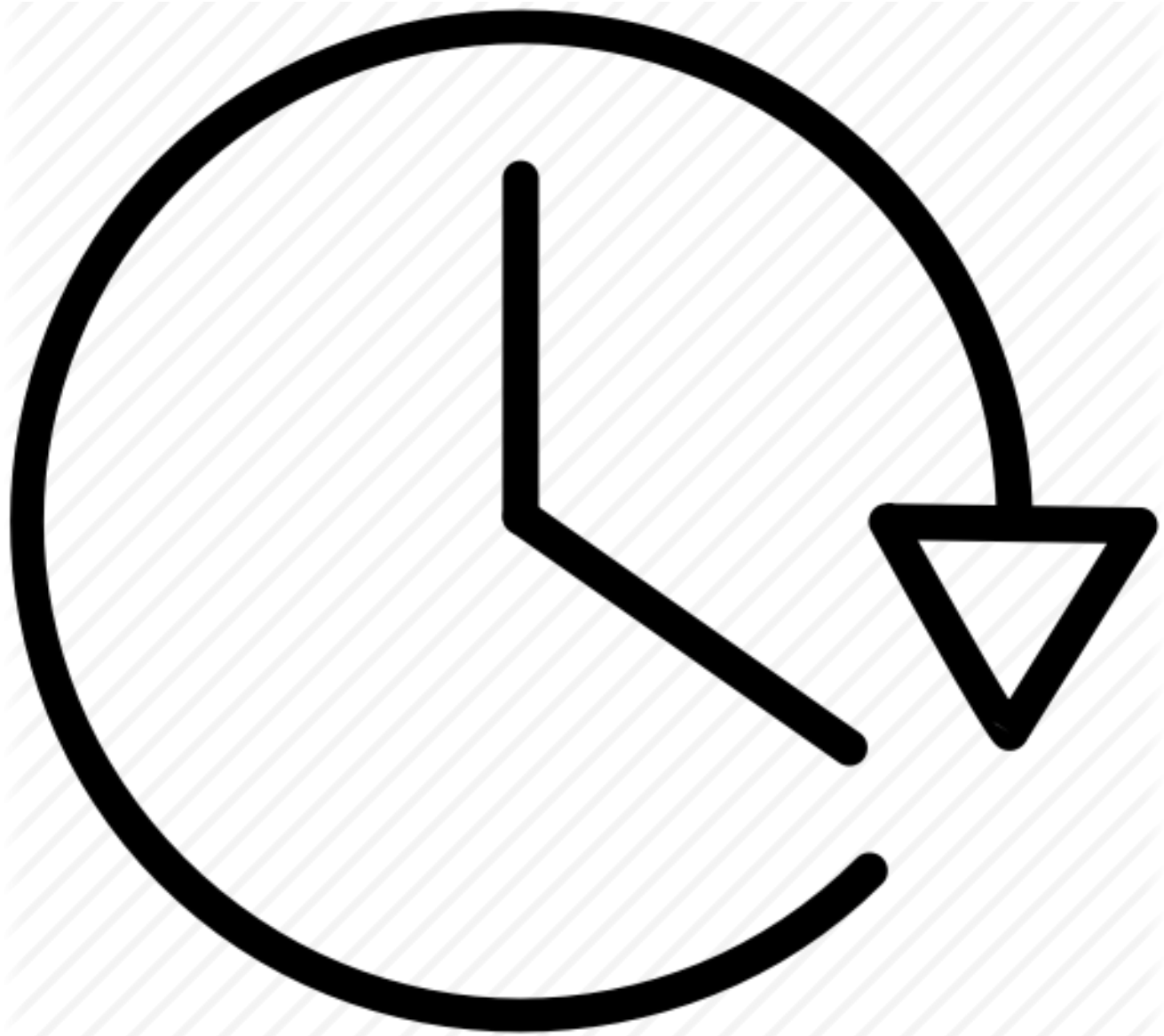
Breakout Question



Suppose you have the opportunity to interview an audit manager (external auditor or internal auditing executive). What questions would you ask?

- _____
- _____
- _____





Report Back



What Question Would you Pose to an Auditor?

Skills

- What real world auditing software tools are used
- What other certifications beside CISA is worth pursuing?

Life of Auditor

- Biggest risk ever found in an audit
- How to handle communication within team and stakeholders of audit
- How to handle communication with those on staff of associate level?
- What is the most common control failure you've seen?
- How to get enough material if client won't cooperate?
- In an audit, what kind of questions will you ask?

Client Relationships

- —
- —
- —

Internal vs. External

- —
- —

Challenges

- What are most common challenges facing IT auditors?



What Question Would you Pose to an Auditor?

Life of Auditor

- How long is the working timeline for a typical project? Does it vary among different industries?
- Are there typical questions (the right questions), auditors always ask clients?
- How do you teach yourself about the business line/group that you're auditing? What resources do you use?
- What is it like in the day of an Auditor (common jobs, assignments)? Is travel common for the job?

Client Relationships

- How do you perform audits in a manner that develops trust? How do they maintain relationships with clients?
- Do you question employees directly with hypothetical questions of how and where would they commit fraud if possible?
- How does an auditor recommend changes to controls to increase buy-in?
- Is it recommended when errors are discovered that auditors help employees correct them before the audit is complete?
- How to document errors without harming relationships (e.g. reduce assistance with future audits)?

Internal vs. External

- What is the difference in the approach of an internal and an external auditor? Are activities coordinated?
- What is the relationship between internal audit and the audit committee?
- How is the effectiveness of internal audit function assessed? To whom does internal audit report ?
- What is relationship of external auditors with the audit committee? How often do they meet?

Skills

- What advice do you give us (grad students in ITACS)? How should we prepare ourselves with little experience in auditing for success in profession?
- What technologic skills should be obtained for IT auditor? Communication skills?
- What are the few key skills/traits successful auditors should have?
- How do you continue to grow within the audit profession?



What Question Would you Pose to an Auditor?

Challenges

- What is the biggest challenge that the company or audit department has gone through?
- What are the biggest challenges in this profession?
- What would you say is the most rewarding part of being on the job?
- How could auditors deliver value to the company?
-
- What kinds of controls is organization most likely to miss?
- What was the most challenging audit you ever worked on? What made it so difficult?
- What is the most challenging problem for the it audit field How is and will technology change the field of auditing?

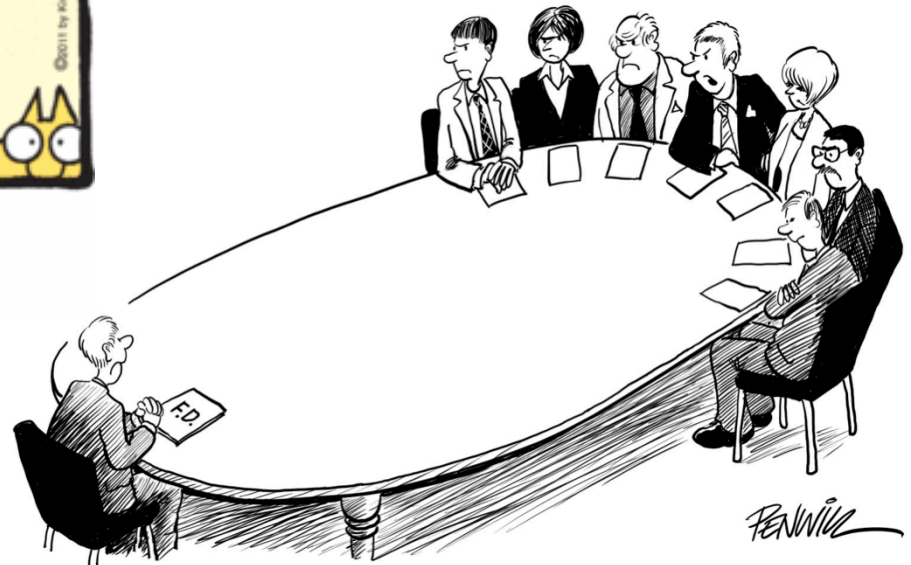


Success with Internal and External Auditing My Personal Experience





"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

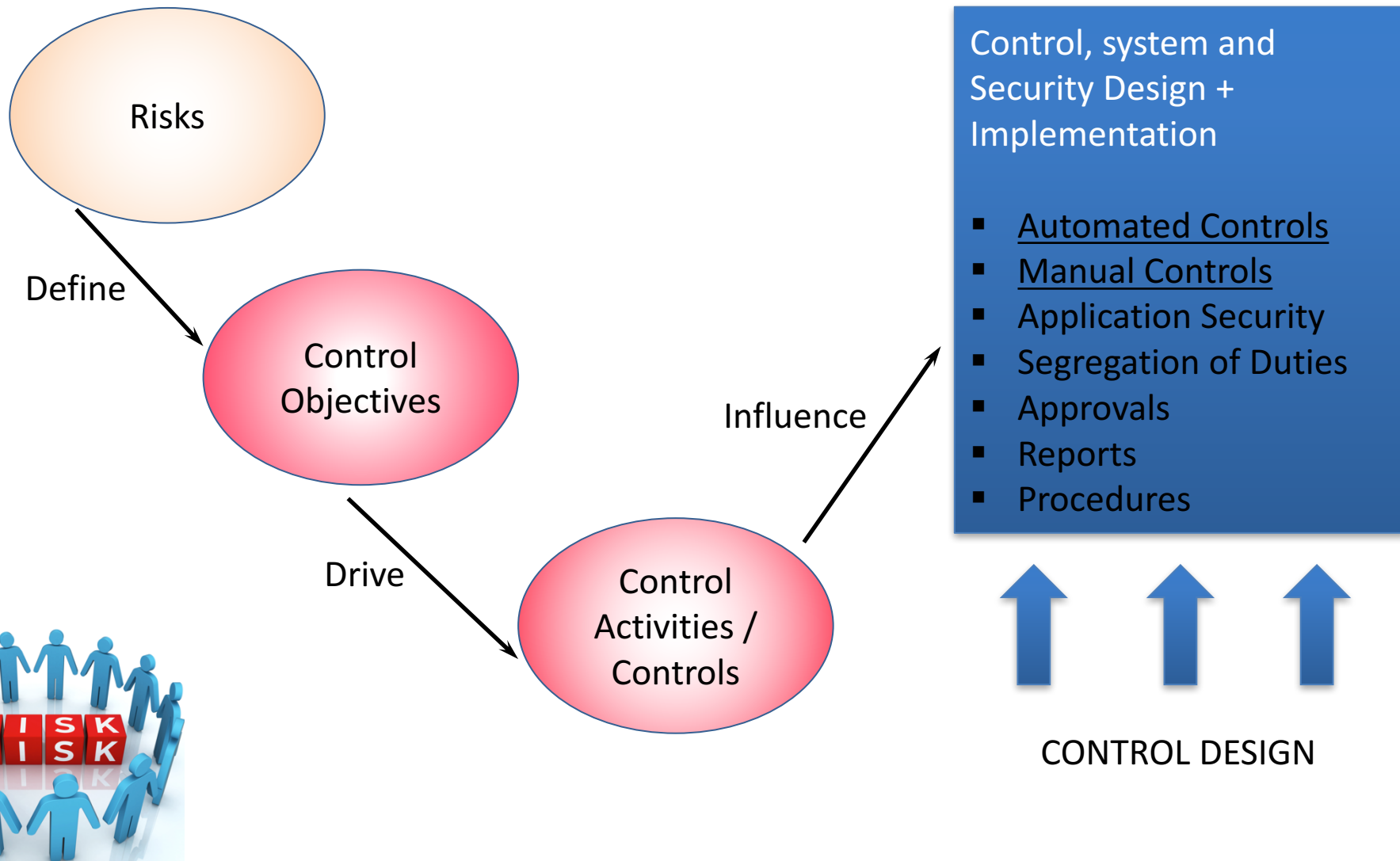




Risk / Control Matrix

Final Exercise

Risk / Control Matrix: Design Approach



Risk / Control Matrix: Final Exercise



- Agenda
 - Last Class (*November 13*): Part 1 (Identify Risks)
 - **This Class (*November 27*): Part 1b, 2, 3**
 - Risk Priority (Severity & Likelihood)
 - Identify Controls
 - Link Controls to Risks
 - Future Class (*December 4*): Part 4 (Complete Control Definitions)
 - Future Class (*December 11*): Part 5, 6 (Control Process / Audit Details; Personal Questions)
 - *Due December 14 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



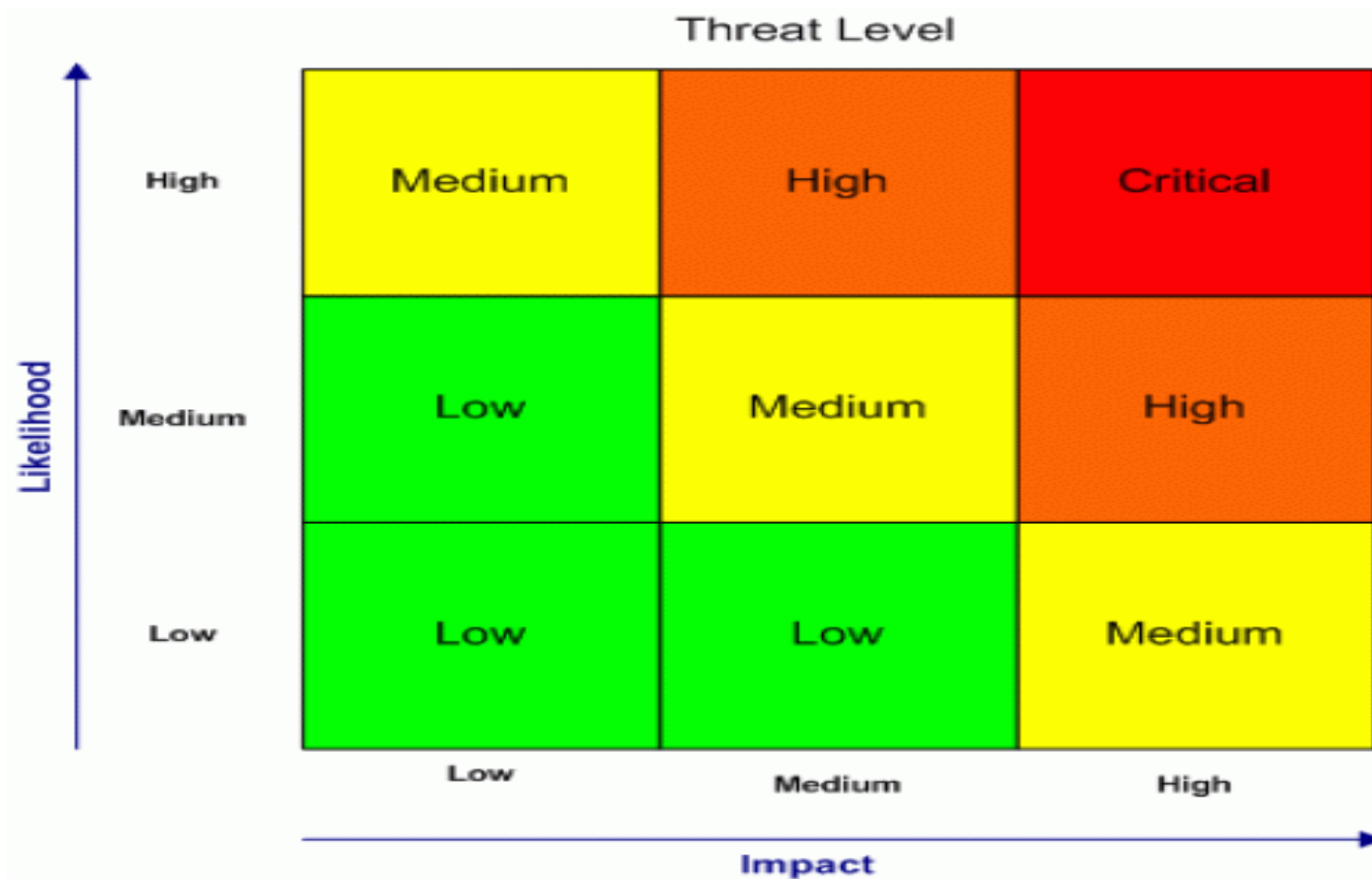
Part 3: Link Risks (Part 1) to the Controls (Part 2)

- 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)

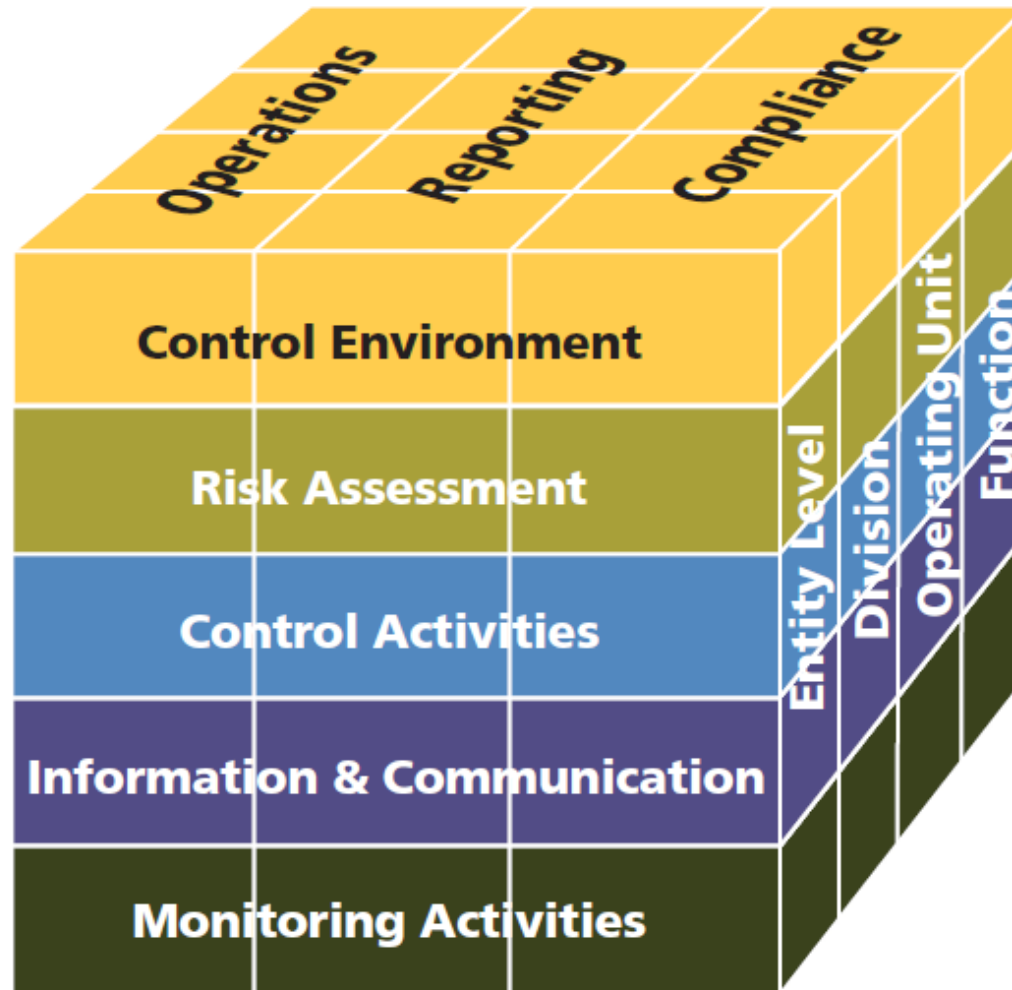


Extra Slides

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

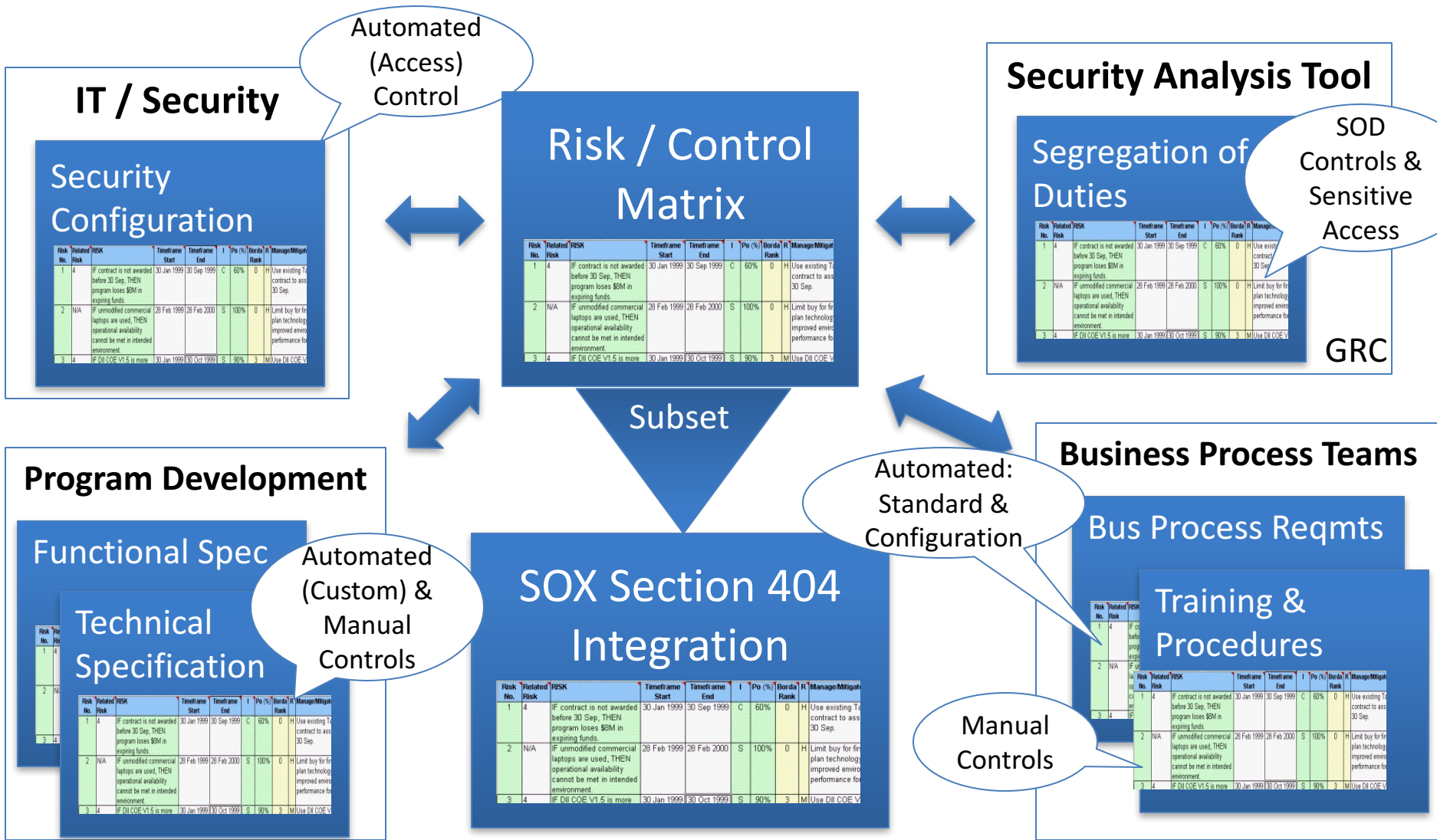
13. Uses relevant information
14. Communicates internally
15. Communicates externally

Monitoring Activities

16. Conducts ongoing and/or separate evaluations
17. Evaluates and communicates deficiencies

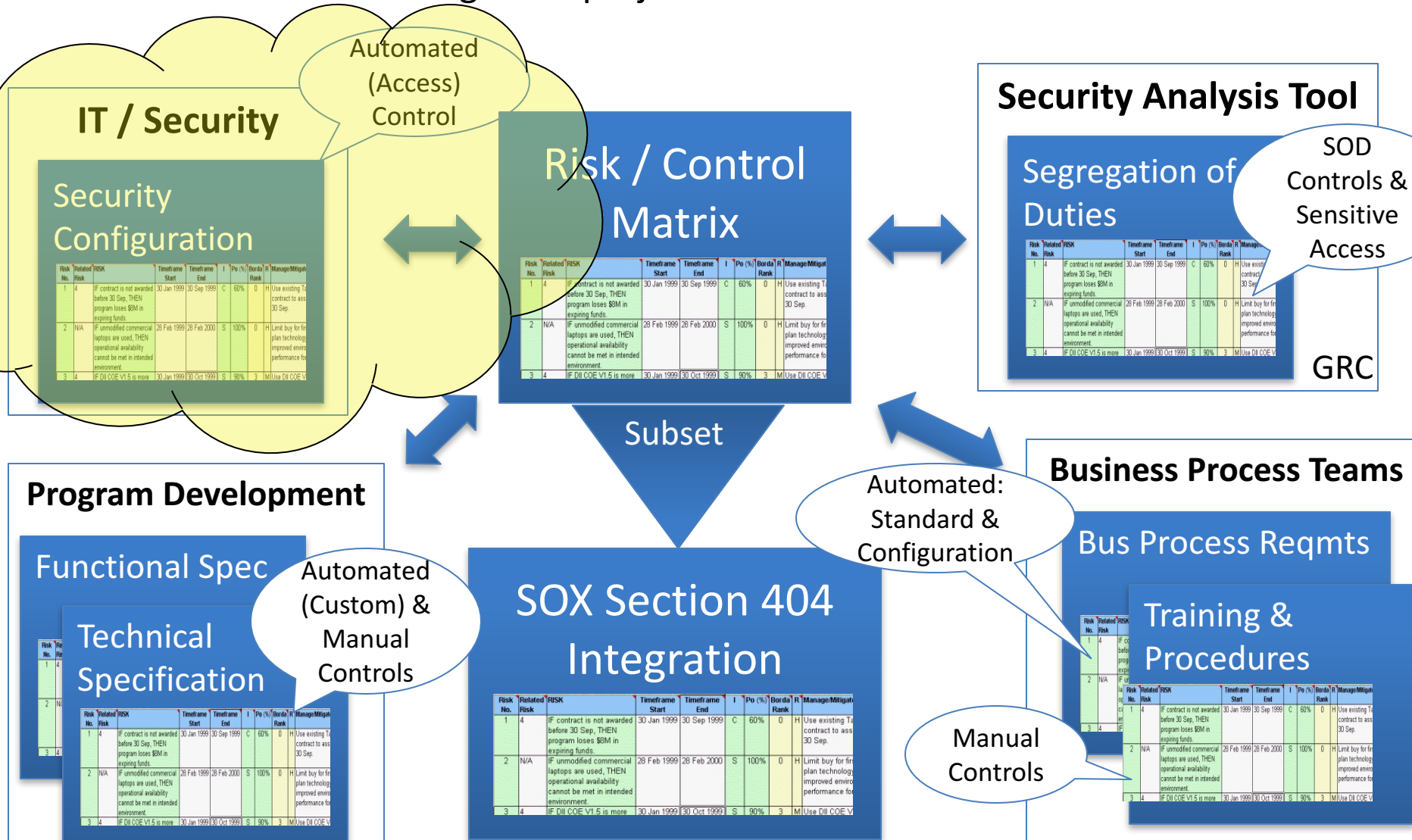
Controls: Integration Points

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.

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 do 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 asses 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?