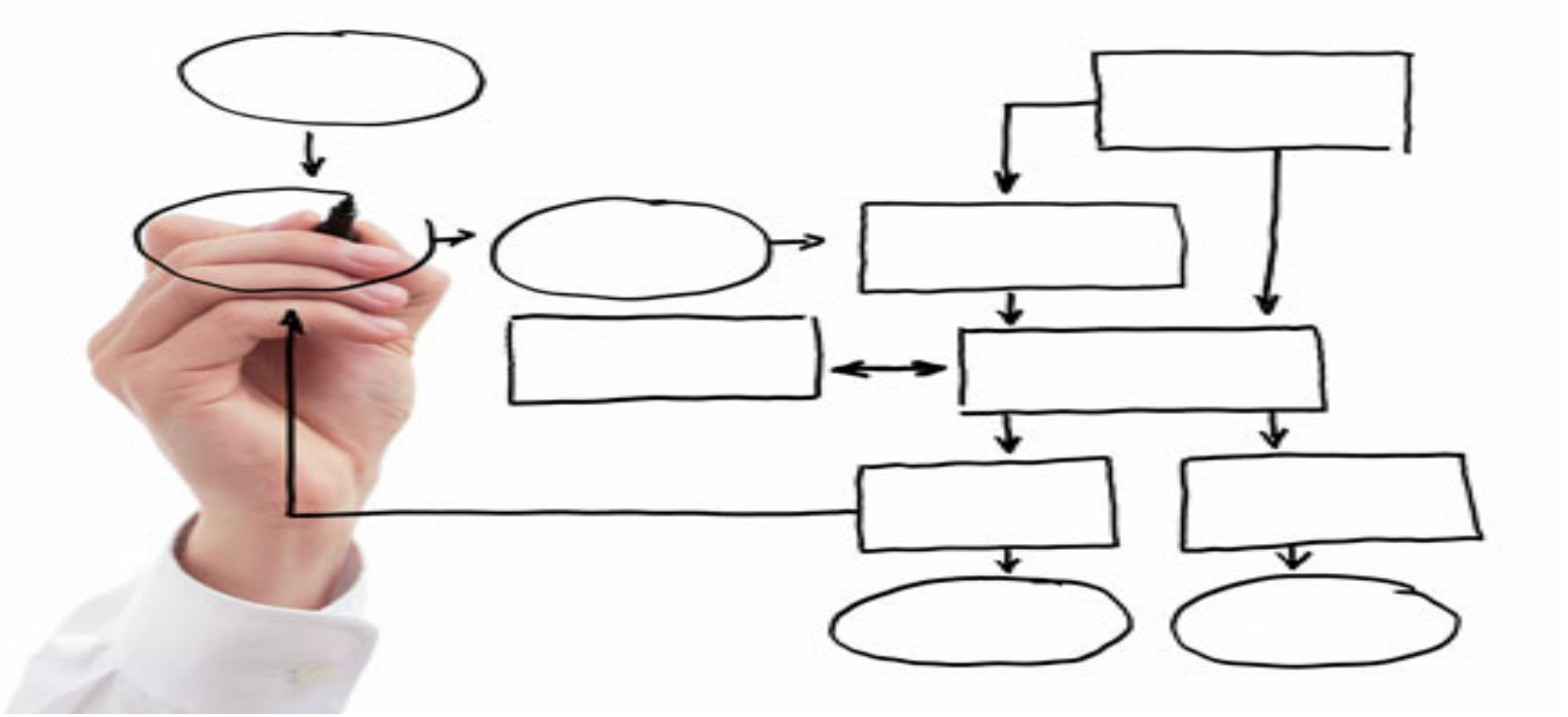


MIS 5121: Business Processes, ERP Systems & Controls
Week 14: *SAP HANA,* GRC, Character

FOX | MIS
Management Information Systems

Edward Beaver
Edward.Beaver@temple.edu
ff

Special Guests

Ray Adams

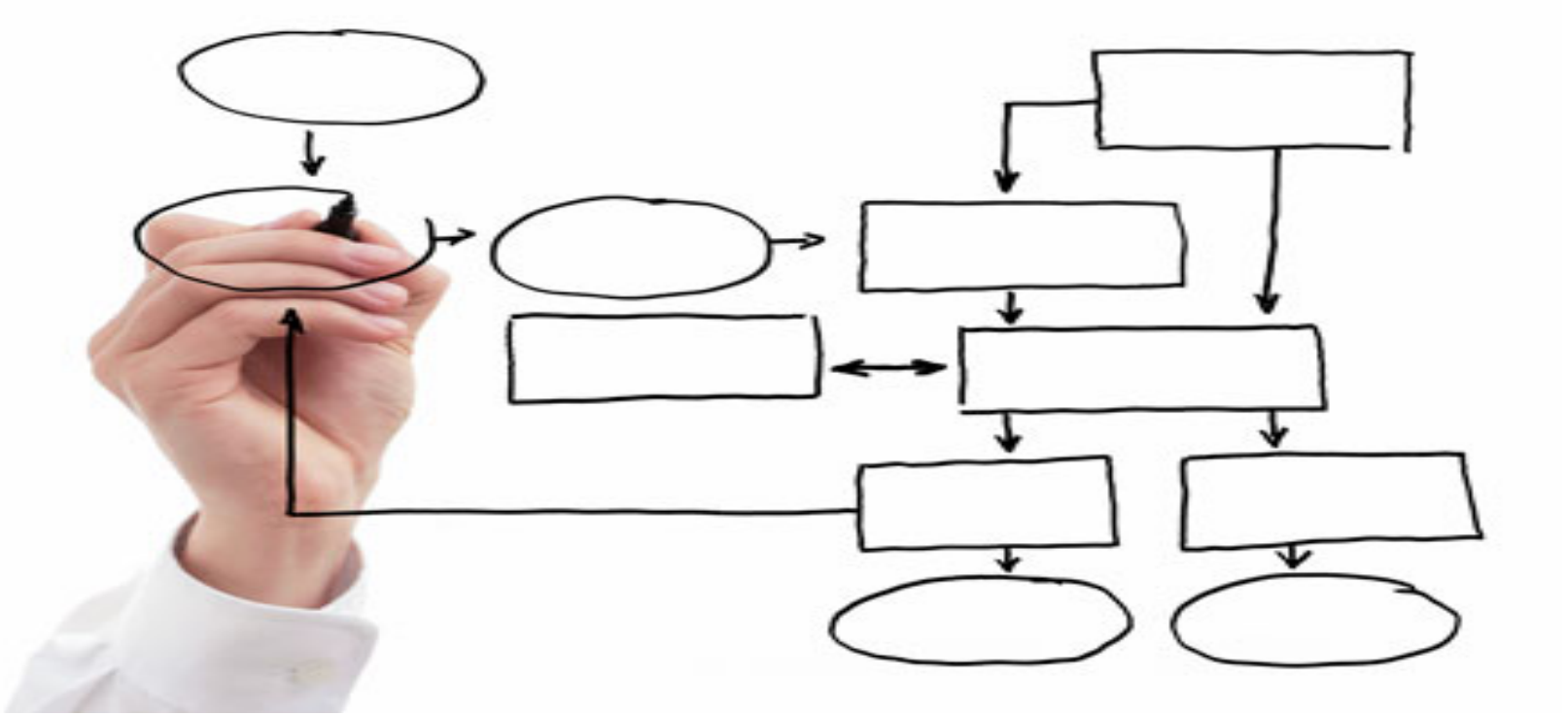
- SAP America, Inc.
- Field Services Director for Industry Business Unit - Chemicals
  (Business and solution development at SAP for the chemical industry)

Dave Moyer

- SAP America, Inc.
- Business Stragegist / Implementation Specialist
- U of Pa / Wharton Alum

MIS 5121: SAP Visit Questions

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



MIS 5121: Business Process, ERP Systems & Controls

Real World Control Failures: Sony (2014)

By: Mickey Majzik

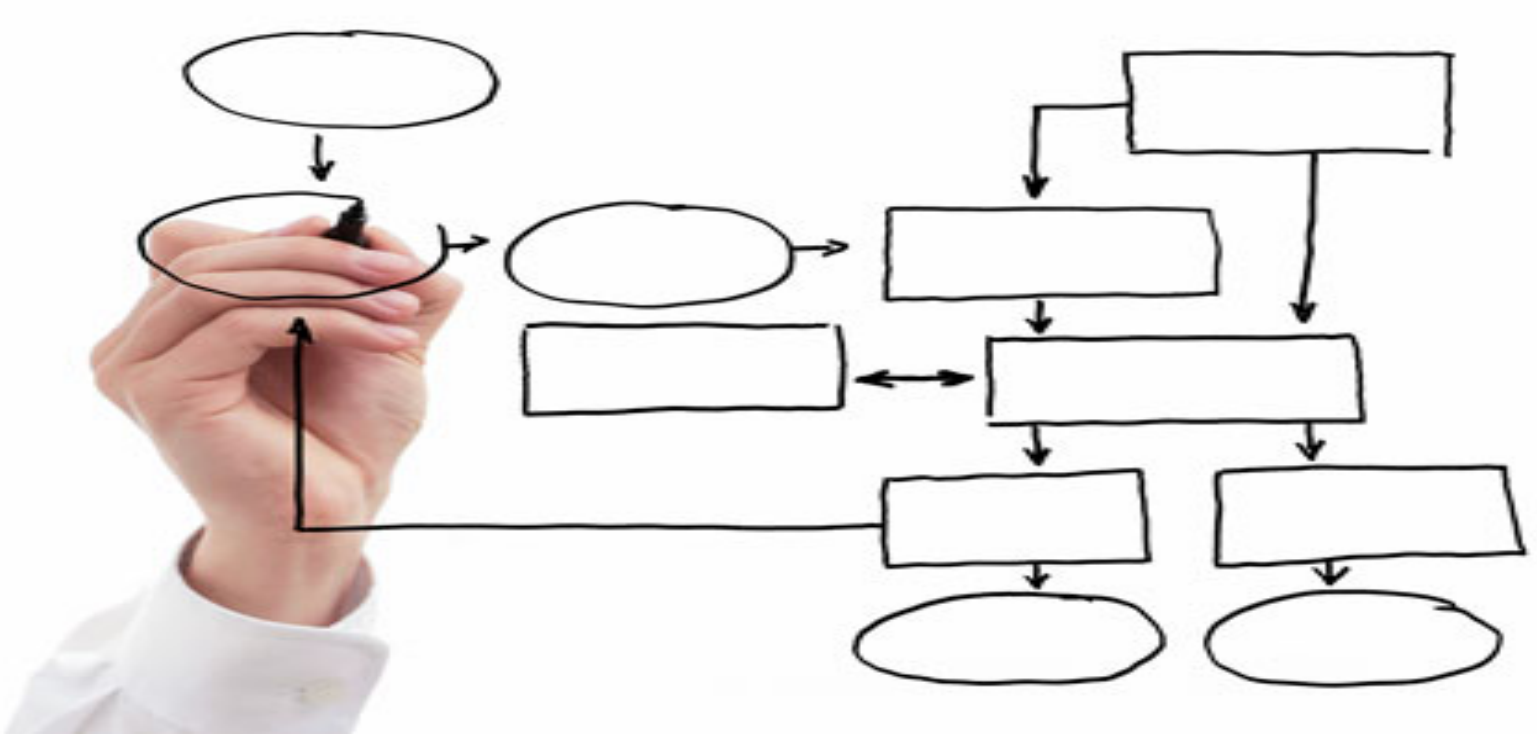
FOX | MIS
Management Information Systems

Control Failure: Network Security

- Background:
  - 2014: Sony Pictures was hacked by a group who called themselves the Guardians of peace
  - Installed wiper malware: Paralyzed the antivirus software and deleted files and documents in the database
  - Released over a dozen terabytes of data and files
- Control Failures:
  - Lack of Intrusion Detection
  - Weak Internal Security Policies
  - Data Classification and Retention policies non-existent
  - Encryption
- Results:
  - $85million in remediation and replacement costs.
  - Damaged Reputation
  - Put an increased emphasis on cyber security
  - Call to action for change
- What Could / Should those in Authority Have Done Different?:
  - Stronger security policies in regards to passwords and data retention
  - Sony may not have been able to prevent they attack, but…
  - Use effective risk analysis

- Reference:

  - (n.d.). Retrieved April 14, 2015, from https://www.capitaliq.com/CIQDotNet/Financial/SegmentsPopup.aspx?companyid=23021&instanceid=1684629508&statekey=f227490cb1de4345afb48d832b85785c
  - Andrew Jaquith. Security Metrics: Replacing fear, uncertainty, and doubt. 2007.
  - ComputerWeekly. Security Think Tank: Lessons to be learned from Sony breach. February 2015. http://tinyurl.com/pqf5vv9
  - Cook, J. (2014, December 16). Sony Hackers Have Over 100 Terabytes Of Documents. Only Released 200 Gigabytes So Far. Retrieved April 14, 2015, from http://www.businessinsider.com/the-sony-hackers-still-have-a-massive-amount-of-data-that-hasnt-been-leaked-yet-2014-12
  - DYADIC. Could the Sony and Anthem hacks have been prevented ? February 2015. http://tinyurl.com/pke7txf
  - eSecurity Planet. Researchers: Sony Hack Was Insider Breach. December 2014. http://tinyurl.com/oqn4k4y



MIS 5121: Business Process, ERP Systems & Controls

Real World Control Failures:

By: Christie Vazquez

FOX | MIS
Management Information Systems

Control Failure: Upcoding scheme and unbundling

- Background:
  - In 2015, Zahar Tkach, also known as Alex Tkach, of Bensalem, PA, was charged by indictment in a scheme to defraud Medicare of approximately $1.25 million by charging for unnecessary ambulance services
  - Tkach owned NovaCare Ambulance and Cardiac Care Ambulance operating primarily in Philadelphia and the surrounding counties
  - Between June 2008 and April 2012, Tkach recruited and transported dialysis patients and conspired to bill Medicare for ambulance transportation services for individuals they knew did not need such services
  - Medicare audited the 2011 billings of Novocare and Cardiac Care
  - Alleged to have obstructed the audits by altering, and directed employees to alter, ambulance transport records and he falsified medical authorization forms

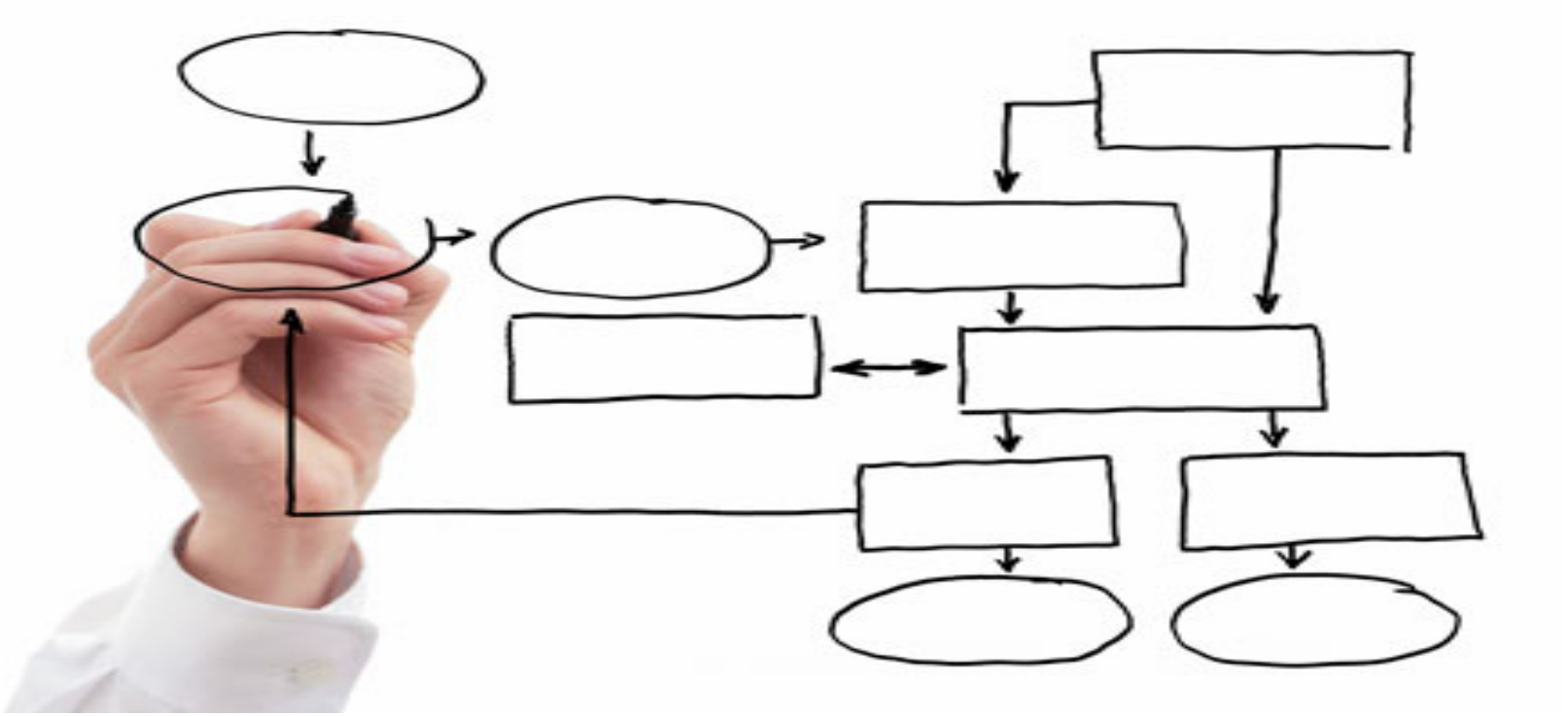
- Control Failures:
  - Vendor management
    - An array of outside contractors used by the government is poorly managed,
  - Inform Medicare recipients of covered and non-covered services
    - Report fraudulent activities
  - Little government oversight

Control Failure: Upcoding scheme and unbundling

- Results:
  - Under an experiment to try to control fraud, the agency now requires advance permission in Pennsylvania, New Jersey and South Carolina for repetitive ambulance rides in cases that are not emergencies
  - Tkach faces up to 10 years in prison for each count of health care fraud; up to five years in prison for each count of obstruction of a federal audit; and 10 years in prison for money laundering. He also faces a possible fine of $250,000 per count

- What Could / Should those in Authority Have Done Different?:
  - Monitored payment for services, especially repeat non-emergency
  - Educate Medicare recipients

- Reference:
  - http://www.bizjournals.com/philadelphia/morning_roundup/2015/09/health-care-fraud-tkach-bensalem-novacare-ambulanc.html
  - https://www.fbi.gov/philadelphia/press-releases/2015/ambulance-company-owner-charged-in-medicare-fraud
  - http://www.nytimes.com/2014/08/16/business/uncovering-health-care-fraud-proves-elusive.html?_r=0



MIS 5121: Business Process, ERP Systems & Controls

Real World Control Failures:

By: _Shizhong Yang

FOX | MIS
Management Information Systems

Control Failure: Toshiba - One of Japan's Largest Accounting Scandal

- Background:
  - Japanese multinational corporation with more than 140-year history.
  - Profits were inflated by $1.2 billion, which is about one-third of Toshiba's pre-tax profits, during the period of 2008 through the third quarter of 2014.

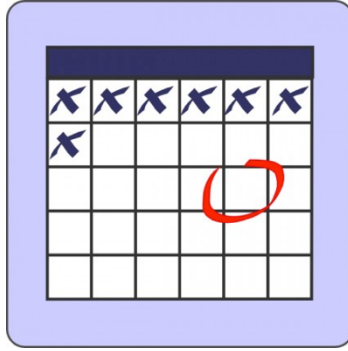
- Control Failures:
  - The fault of the internal audit in Toshiba was that it focused on consultation service rather than assurance service.
  - The audit committee was neither capable nor independent.
  - Internal audit function relied excessively on rotational staffing that at times left it vulnerable in terms of resources and competency.

- Results:
  - The resignations removed half of Toshiba's 16-member board.
  - Some shareholders are expected to file a class-action lawsuit against the firm.
  - Japanese market will lose the trust of overseas investors.
  - $4.5 billion loss in 2015 to deal with the aftermath of a massive accounting scandal.(Result from restructuring costs, poor performance from the company's energy and electronic devices divisions and income tax payments.)
  - The scandal news drove the stock price down 11% by the end of the trading day in Tokyo.

Control Failure: Toshiba - One of Japan's Largest Accounting Scandal

- What Could / Should those in Authority Have Done Different?:
  - Heads of internal audit must have a keen understanding of their organizations' risk tolerance, what their organizations expect of the internal audit function, and whether they have the resources and skill levels on staff to meet those expectations.
  - Auditors must keep in mind their role in auditing corporate culture.
  - The audit committee should be capable, independent, and effective.
- Reference:
  - http://www.japantimes.co.jp/news/2015/09/18/business/corporate-business/pressure-to-show-a-profit-led-to-toshibas-accounting-scandal/#.Vx1wpqgrIUU
  - http://www.business-standard.com/article/opinion/toshiba-a-case-of-internal-audit-failure-115080900760_1.html
  - http://www.nytimes.com/2015/07/22/business/international/toshiba-chief-and-7-others-resign-in-accounting-scandal.html?_r=0
  - http://www.iia.nl/actualiteit/nieuws?newsId=1971

MIS 5121: Upcoming Events

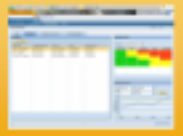


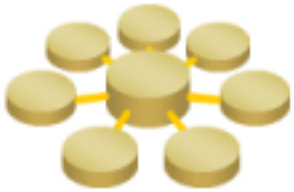
- Reading Assignment 9 – *Due: Yesterday*
- Guest Lecture: SAP What's New (HANA) - *Today*
- Final Exam - *May 2*
  - Similar in format to Exam 1 and 2
  - 6 pages of notes allowed (whatever format)
  - Content
    - Since Exam 2
    - Prior topics outlined in Week 12 and 13

GRC – Governance, Risk & Compliance

SAP BusinessObjects Solutions for Governance, Risk and Compliance

SAP GRC Risk Management





Risk Repository

- Risk Registry
- Links Risks and Controls
- Cisco SONA & Business Process Monitoring

Access Control | Process Control | Environment/Safety | Global Trade | SONA/GRC xApp

SAP NetWeaver — Business Process Platform — CISCO SONA

Sources

ORACLE | PeopleSoft | SAP | Legacy

External Provider | KRIs / Content

A Corporate Platform for Governance, Risk & Compliance

Automates and embeds GRC processes into business processes

GRC: Governance, Risk & Compliance

- History / Structure
  - ‘Virsa’ – Purchased S/W, ran in ECC address space as an ‘add-on’ (based on PWC tool)
  - 2006 SAP bought Virsa, upgraded and released as v5.3 – separate Net-Weaver module
  - SAP GRC v10.0 - Major overhaul

SAP SECURITY & GRC ®

GRC: Components

SAP SECURITY & GRC

GRC: Governance, Risk & Compliance

Modules (Access Control)

SAP v5.3	SAP v10.0	Function
Risk Analysis & Remediation	Access Risk Mgmt (ARM)	- SOD Rule Set (Starter rules) - Analyze and manage Access and SOD Risk (SOD, SAT Reports) - Role / User level simulation
Compliant User Provisioning	User Access Mgmt (UAM)	- Access Request & Workflow - Provision and Manage Users - Business Rules
Enterprise Role Mgmt (ERM)	Business Role Governance (BRG)	- Role Configuration - Maintain Roles (owners, mass change) - Integration with ARM prevents SOD conflicts

SAP SECURITY & GRC ®

GRC: Governance, Risk & Compliance

Modules

SAP v5.3	SAP v10.0	Function
Superuser Privilege Mgmt	Central Emergency Access (CEA)	- Firefighter administration and access portal - Can cross SAP and other apps - Sub-process of Access Control
	Process Control	- Manage developing control process documentation - Automated control testing & monitoring - Documentation from risk / control matrix
	Risk Management	- Risk ID, scenarios - Assessment of risk (indicators) - Risk response

SAP SECURITY & GRC ®

GRC: Governance, Risk & Compliance

Key Benefits

- Real-time analysis of SOD and SAT violations
- Possible automation of compliance requirements (SOX, FDA, etc.)
- Transparency of risks – align with strategic priorities and business objectives
- Proactive monitoring (centralized risk indicator framework)
- SAP integration makes implementation, maintenance easier (lower cost)

SAP SECURITY & GRC ®

Assignment Questions - GRC

- What are the purposes of integrated GRC approach?
- What are potential risks or weaknesses when implementing the integrated approach in SAP?
- Is it impossible to detect authorization risks without using tools?
- What does automating the GRC process mean? Does content automation primarily mean reducing administrative effort required by people responsible for compliance?
- How does automated ICS process cooperate with the comprehensive GRC approach?
- What is the relationship between SAP process control and ICS framework?
- In the Policy Management component, what is the entire life cycle of a policy?
- Does User Access Review happen every time when a user accesses to the system? Who is responsible to the UAR?
- What type of compensating controls we can have for access controls?
- It was unclear if UAM in SAP can provision accounts in other applications and provide the capability for an enterprise user account management provisioning tool?
- How is the risk matrix constructed in SAP GRC Tool?
- GRC may be important and effective, but can the cost of GRC be justified?

Key IT Controls Overview

- GRC
  - What is means
  - 2-3 Functions Included
  - 1-2 Benefits of Use

SAP SECURITY & GRC ®

Character


Self-Control
Respect
Excellence
Honesty
Responsibility
Courteous

Character and Controls

Character:

the mental and moral qualities distinctive to an individual
(Oxford Dictionary)

Who you are when no one's looking

Decisions made in moment of moral crisis shows our true character and morality.

In the Real World Control Failures we've reviewed, Describe the character of the leaders involved (a root of the control failures)?

_____

Character and Controls

What are the differences between the ‘Adams’?

- Adam I - ‘Big Me’
  - _____
  - _____
  - _____
  - _____
- Adam II - ‘Little Me’
  - _____
  - _____
  - _____
  - _____

Character and Controls

- Adam I - 'Big Me'
  - Career-oriented: build, create, produce
  - Ambitious – "Success"
  - Selfishness – has infinite desires
  - Economic logic – cultivate your strengths
- Adam II - 'Little Me'
  - Internal: moral qualities, right vs. wrong
  - Sacrifice self in service to others "Charity, love and redemption"
  - Moral logic - give to receive
  - Humble
    - Wisdom isn't a body of information. It's the moral quality of knowing what you don't know and figuring out how to handle your ignorance, uncertainty and limitations.
    - Go down to go up – valley of humility to climb heights of character
    - Basis for grace

Character and Controls

Which Adam does Culture nurture?

Which Adam are you?

Character and Controls

Which Adam does Culture nurture?

Adam I - 'Big Me'

- Be the best you can be
- Natural disposition (self)
- Adam II - 'Little Me' has been displaced by Adam I – 'Big Me'
- Mental space once occupied with moral struggle has become occupied with struggle to achieve

Character and Controls

Which Adam are you?

My Take Aways:

- Character is on the inside
  - Not what we do
  - But directly shapes what we do
- OK to be flawed – we all are.
- Character can be developed
  - Face our imperfect nature with humility
- Move from Success to Significance (Deep Satisfaction)
  - No good life is possible unless it's organized around a vocation, not serving ourselves. Look outside yourself for a problem / opportunity addressed by an activity you intrinsically enjoy

Character and Controls

Humility Code

- We're not wired to live for happiness, we live for holiness
- Holiness defines the goal of life – at our core we're flawed
- Although we are flawed creatures, we are splendidly endowed
- Pride is the central vice
- Character is built in the course of our inner confrontation
- Things that lead us astray are short term – Character endures for the long term
- We cannot achieve self-mastery on our own – we need redemptive assistance from outside (God, family, traditions, …)
- No good life is possible unless it's organized around a vocation – a problem addressed by an activity you intrinsically enjoy
- Person who successfully struggles against weakness may or may not become rich and famous, but that person will become mature

David Brooks: The Road to Character

Assignment Questions - Character

- What mindset is more helpful in being successful; being humble or more self-absorbed and concerned with yourself?
- Do you think self-awareness can be practiced or not? If possible, how to practice?
- In the valley of humility they learned to quiet the self. However, when you facing difficulty or disaster, how can you overcome the fear can see the world clearly?
- **In your life, have you faced any hardships, and what did you do to overcome those hardships to make yourself better?**
- How to make you not only grateful or humble in respect to others but also make you realize who you really are?
- Why it is importance of practicing small acts of self-control?
- *What are some examples of their road to character?*
- Life stories of persons in book show how they met diversity and rose to a level of success. However, what toll did their journey have on the family and how did they cope?
- Which character is more suitable for the current society, big me or little me?
- *A person's character is very crucial in the audit industry. How do we build our reputation and maintain a good ethical character in this industry?*
- **How would you define " eulogy virtues" and "resume virtues"?**
- Is there something that a person should change in themselves to build character?

Professor Ed Beaver

Thoughts on Success

(Gleaned from my 39 Year Career)

'The wisdom of moderation is not just realize the midpoint between two opposite poles, but instead, it is an awareness of the inevitability of conflict.'

Success . . . First Things First

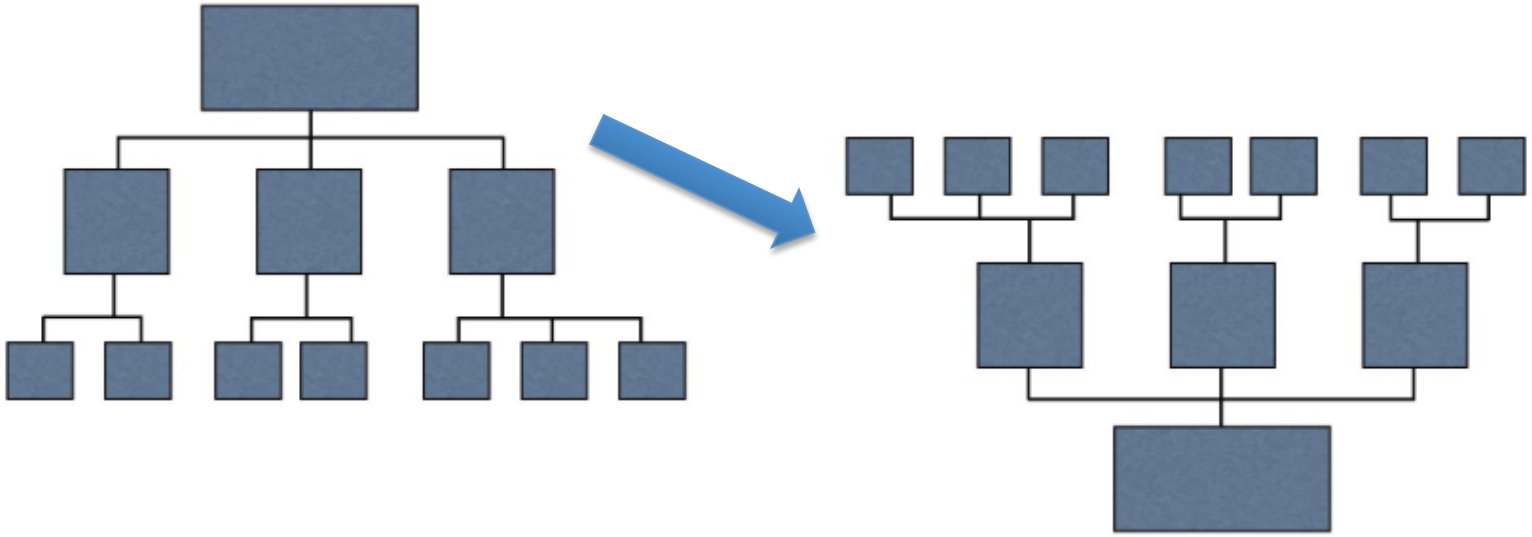
- Solve Business Problems
  - Learn all you can about the business
  - Outcome is business success / value
- Right role of Technology (IT and SC)
  - Technology is Fun
  - Business Value is the end – not Technology (Beware of technology driven initiatives)

Success . . . Your Personal Act

- Whatever our Job / Role is – Do it Well
- Interpersonal Skills are Critical – hone them
  - Speak and write well
- Be Inquisitive, Learn Continually
- Energy – in all you do, ,exude it
- In your career you'll have many bosses - some good, some bad. Manage the relationship
  - Boss knows what you're working on – contributions
  - Boss working to support your efforts

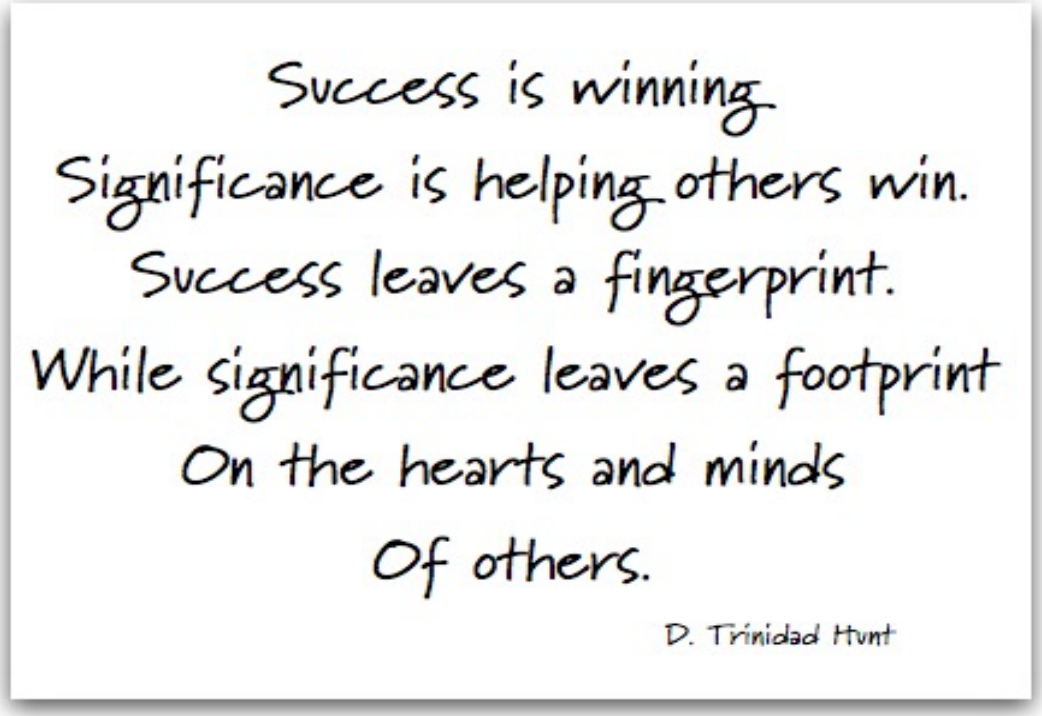
Success . . . Beyond Yourself

- Team
- Leadership
  - Vision
  - Other Focus



Success . . .

- Initial Focus in life (business) - *Success*
- Later focus of life (personal) - *Significance*
  - More to life than work – work / Life balance
  - Me
    - Faith
    - Family



Ref: Halftime book by Bob Buford

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**

Risk / Control Matrix: Final Exercise

Part 5: Create Control Process and Auditing Documentation for the Order to Cash (OTC) process

- Appendix 2 and 3 of the Exercise Guide has documentation examples from the Procure to Pay process:
  - Appendix 2: Automated Configuration Control
  - Appendix 3: Manual Monitoring Control
- Using these examples and format, create **one** example document for one of your identified OTC Controls (Part 3)
- Submit as separate Word document or insert as tab in Submission Spreadsheet
- Resources:
  - Professor: in class, e-mail, phone (609-206-9783)
  - Table TSTC (List of transaction codes – reports)

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

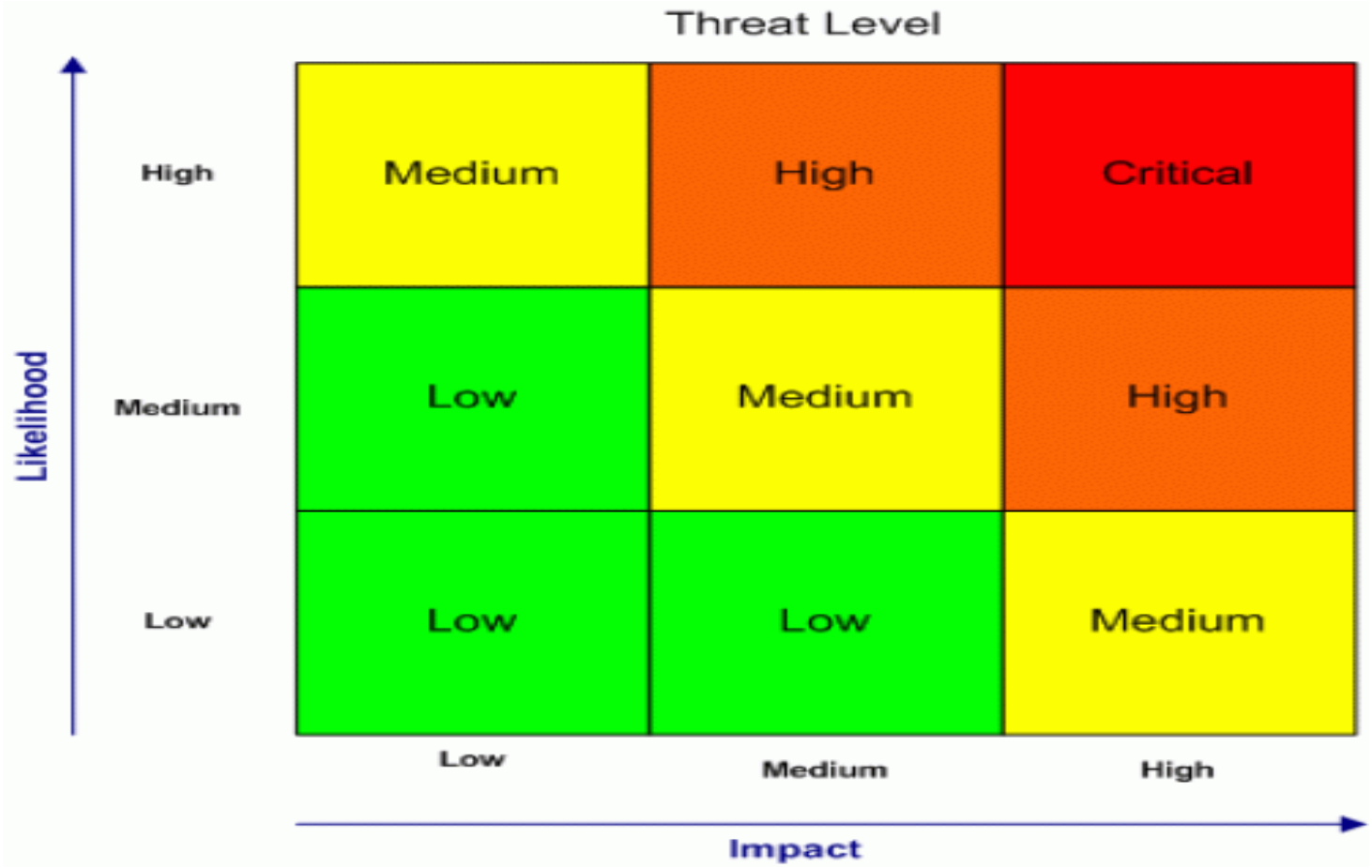
- Tab: Part 2 – GBI Controls
- Identify at minimum 15 controls for the process
- Identify a minimum 3 controls in each of the OTC sub-processes:
  - ✓ **OR&H**: Order Receipt and Handling
  - ✓ **MF**: Material Flow (shipping)
  - ✓ **CI**: Customer Invoicing
  - ✓ **PR&H**: Payment Receipt and Handling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

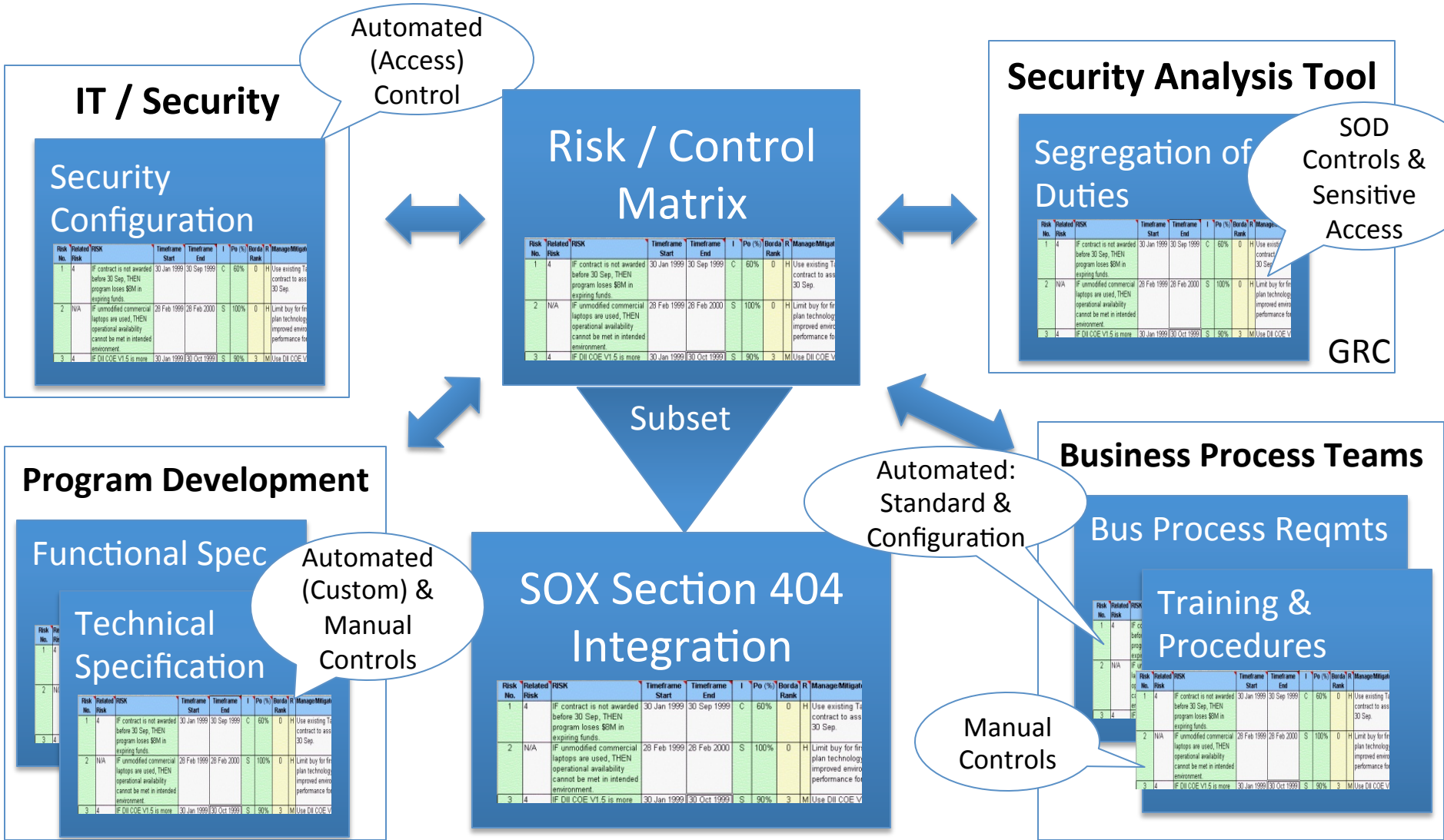
Control, system and Security Design + Implementation

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

CONTROL DESIGN

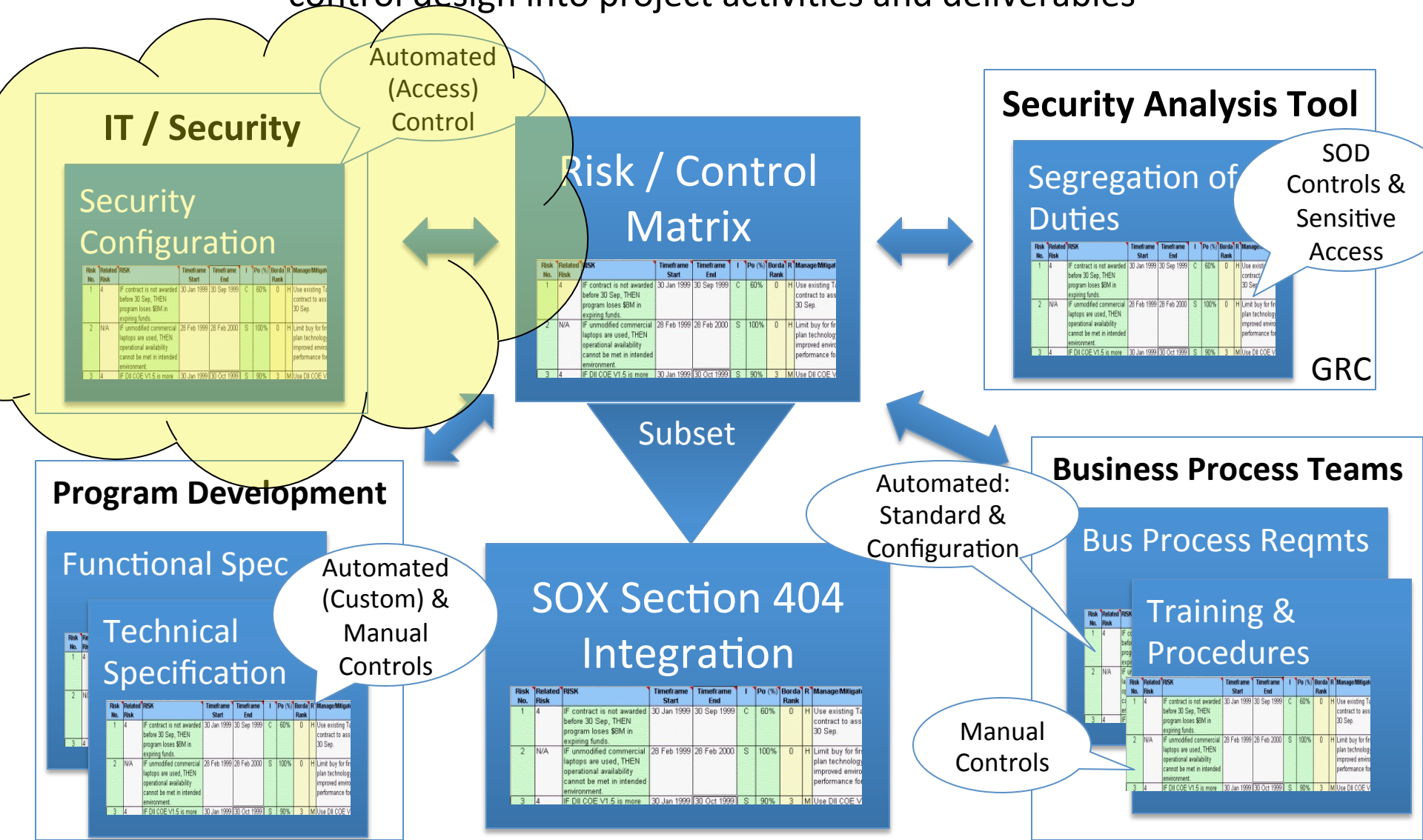
Controls: Integration Points

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

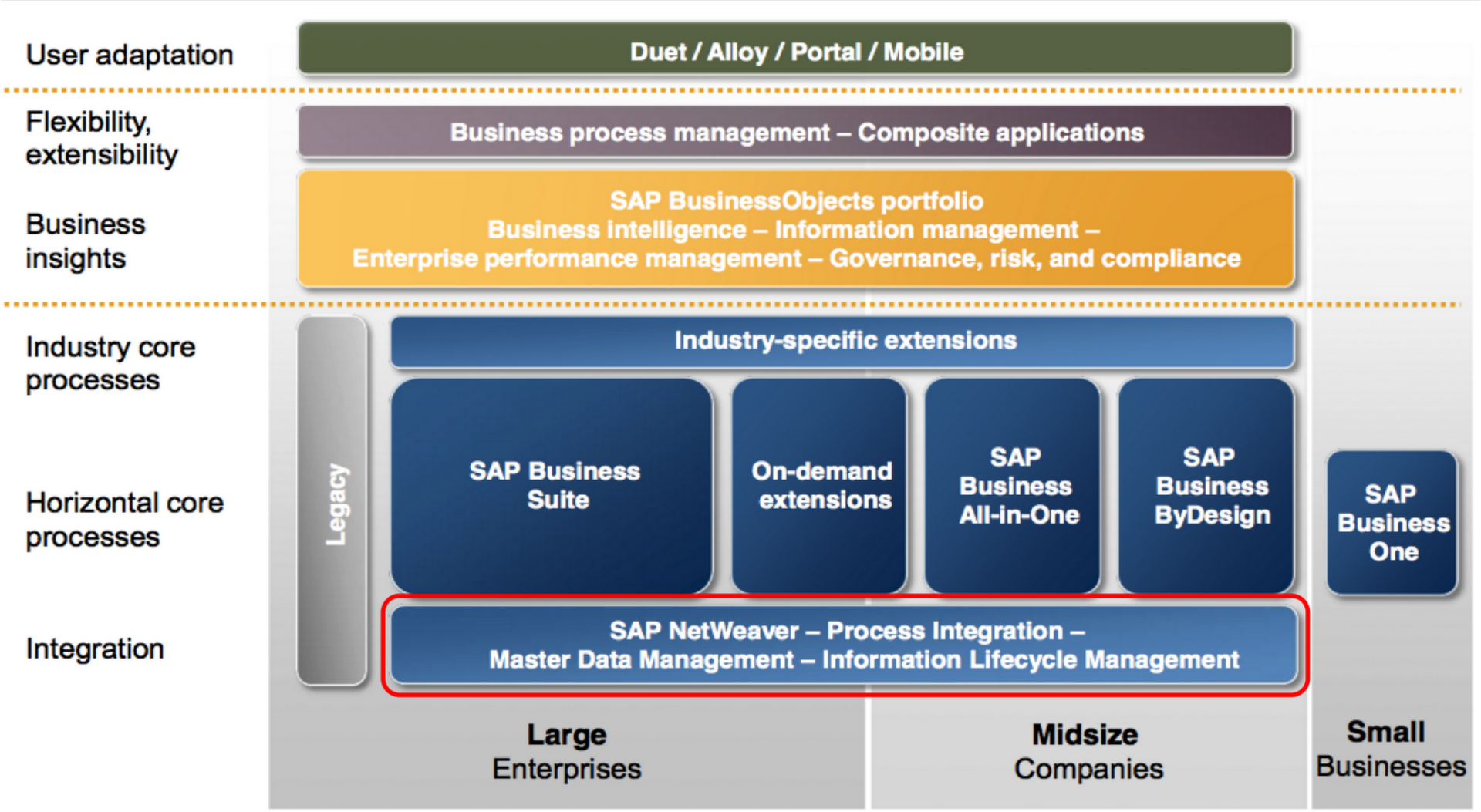


Controls: Integration Points

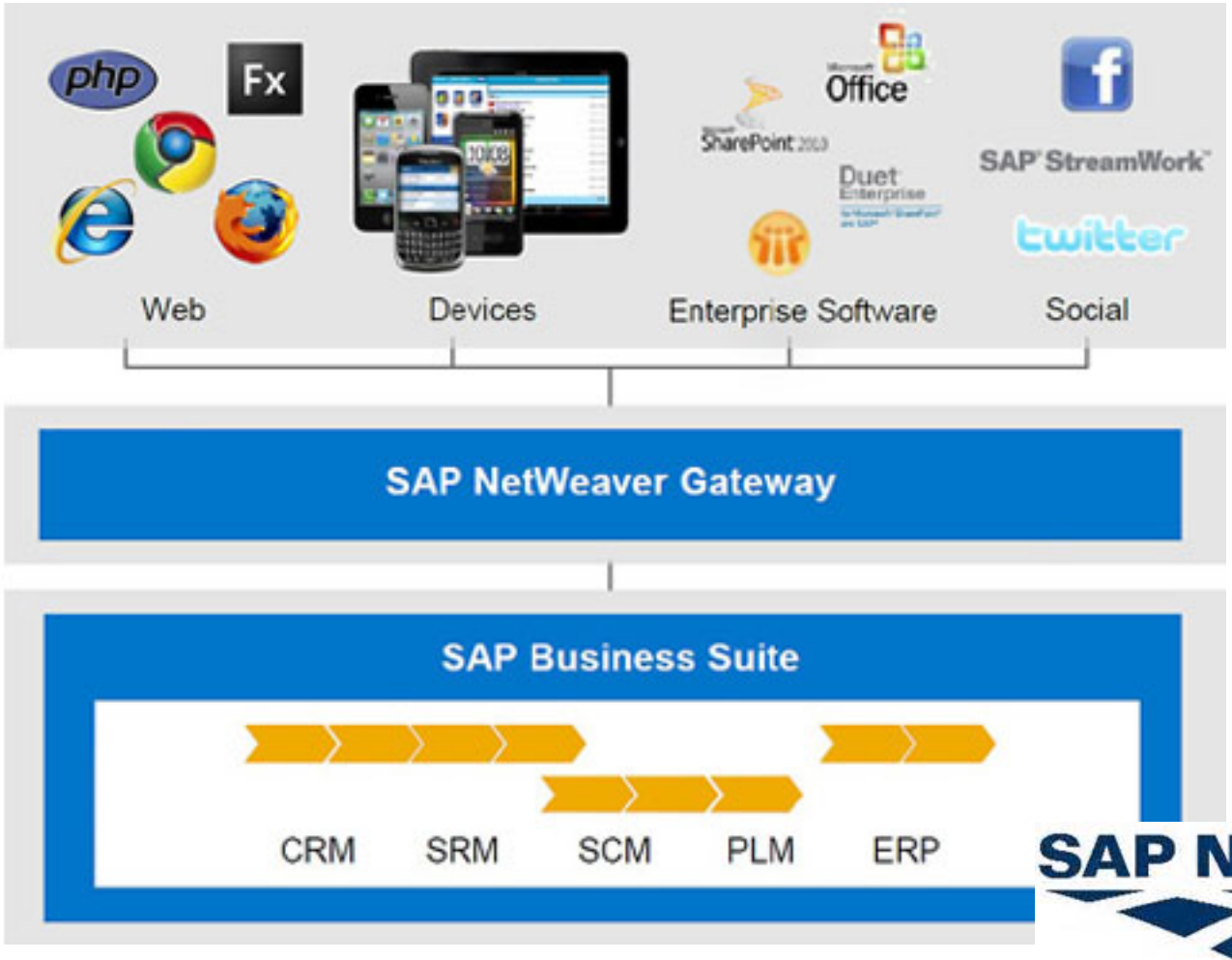
Risk/Control Matrix can serve as the primary vehicle for integrating control design into project activities and deliverables



SAP: Not Just ECC/ERP



SAP: Business Suite



‘The wisdom of moderation is not just realize the midpoint between two opposite poles, but instead, it is an awareness of the inevitability of conflict.’