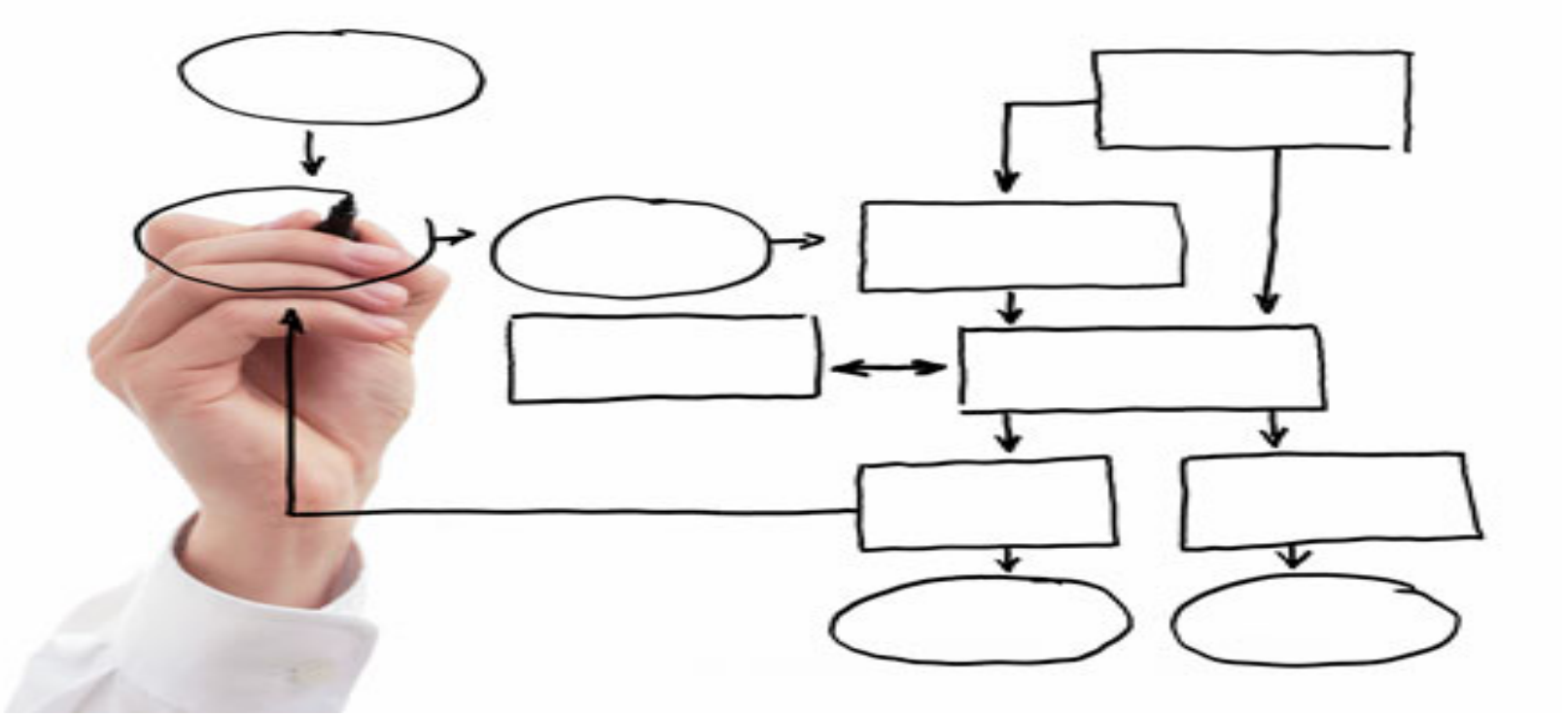


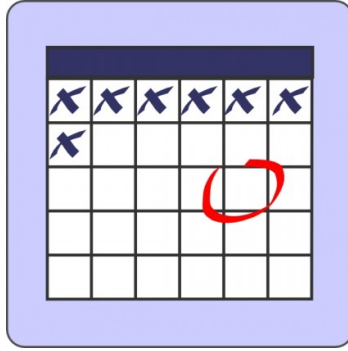
MIS 5121: Enterprise Resource Planning Systems

Week 13: *SAP's GRC Module; Emergency User; Other SAP Module Security*

FOX | MIS
Management Information Systems

Edward Beaver
Edward.Beaver@temple.edu
ff

MIS 5121: Upcoming Events



- Reading Assignment 9 – *Past Due: April 19*

- *April 20 Class:* Firefighter, GRC, Other SAP Module Security
- *April 27 Class*: Few loose ends; Review and Exam Guide, Your Q&A

- Extra Credit Opportunity (Optional) - *Due: April 28*
- Final Exercise (Risk/Control Matrix) – *Due: April 30*

- **Exam 3** – In class*: May 4*
  (Potential conflict with Capstone Class Resolved)

MIS 5121: Question & Answers

During Class Next Week (April 27)

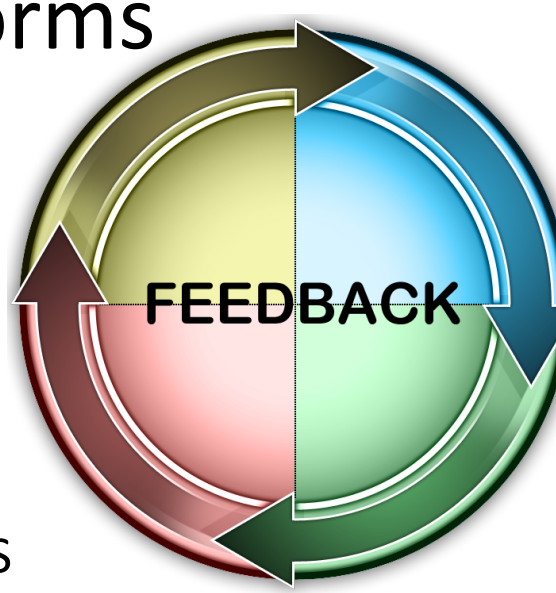
- Your chance to ask me questions related to course topic - I'll attempt to answer or get you an answer

- *Each person must ask minimum of 1 question*

- **Recommendation:** review all your assignments and chose 2-3 questions still unanswered

  (2+ because others may ask your same questions)

SFF: Student Feedback Forms



- Value
  - ❖ Your feedback already (after tests, etc.) has already helped me improve the class
  - ❖ You wouldn't have Exam Guides for Exam 3 without your feedback
  - ❖ Better class for subsequent students and to FOX MIS in total

- Request
  - ❖ Have received the e-SFF e-mail??
  - ❖ Take 10-15 minutes to complete: next class
  - ❖ http://esff.temple.edu

Control Failure: Ibtissam Bazzine

- Background:
  - ❖
  - ❖
- Control Failures: 2006 – 2009
  - ❖
  - ❖
- Results:
  - ❖
  - ❖
- Reference:
  - ❖

Control Failure: Pavel Sasna's Presentation

- Background:
  - ❖
  - ❖
- Control Failures: 2006 – 2009
  - ❖
  - ❖
- Results:
  - ❖
  - ❖
- Reference:
  - ❖

Control Failure: Michael Roth's Presentation

- Background:
  - ❖
  - ❖
- Control Failures: 2006 – 2009
  - ❖
  - ❖
- Results:
  - ❖
  - ❖
- Reference:
  - ❖

Key Information Technology Risks

- **System Security**
- **Information Security Administration**
- **Logs and Traces**
- **Instance Profile Security**
- **Change Management**
- **Transport Security**
- **Change Control**
- **Data Migration**
- **Data Interface**
- **Table Security**
- **Data Dictionary, Program and Development Security**
- Powerful User ID's and Profiles
- Firefighter access

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 ID's and Profiles

Risks:

- SAP_ALL 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 and Profiles

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

- Standard User IDs in all SAP installations
- Come with predefined names and passwords
- Need to be protected with password changes
- Companies should develop Policies and Procedures for their usage and monitoring

SAP Default IDs

DDIC

- Special privileges for software logistics and ABAP/4 dictionary
- Automatically created when clients 000 and 001 created
- Required for certain installation and setup tasks
- Do not delete DDIC master record in Client 000

SAPCPIC

- Cannot log on in dialog
- Allows the SAP system to call programs and function modules
- Allows EarlyWatch to collect performance data, execute external background programs and retrieve values for the Computing Center Management System (CCMS)

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:

- 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 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:
  - 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 to users while creating an auditing layer to monitor and record Firefighter usage
  - Reason for emergency use
  - Date / time stamps
  - What Transactions were used
  - Which updates made

- Transaction: /n/VIRSA/VFAT

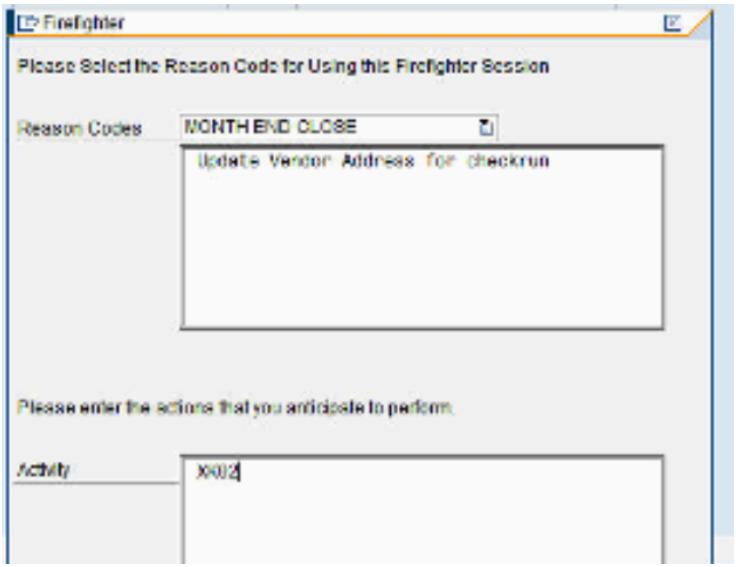
Firefighter (FF) / Emergency User

- Access:
  - ECC Transaction: /n/VIRSA/VFAT
  - GRC Module

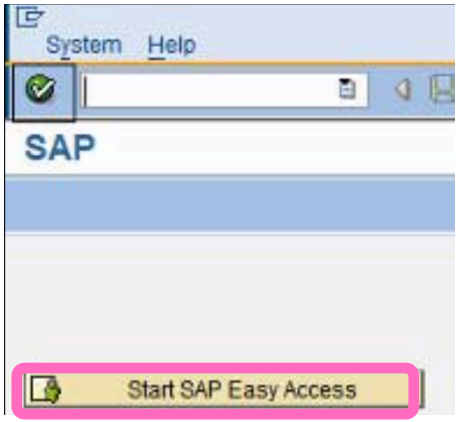
- Logging On creates a new SAP session as if the FF ID had logged on.

Firefighter (FF) / Emergency User

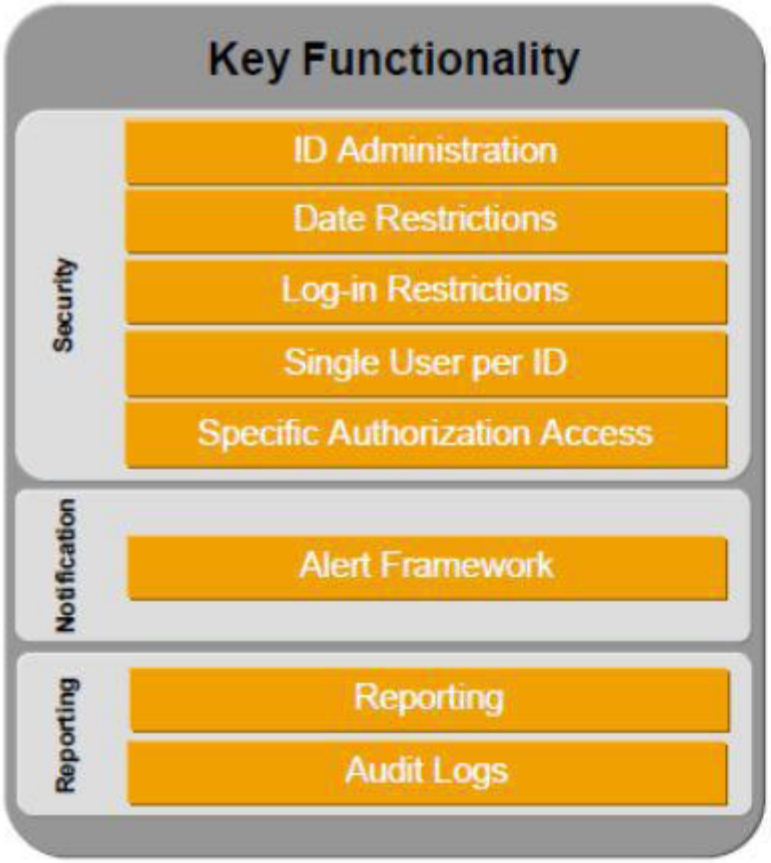
- Reason for access:

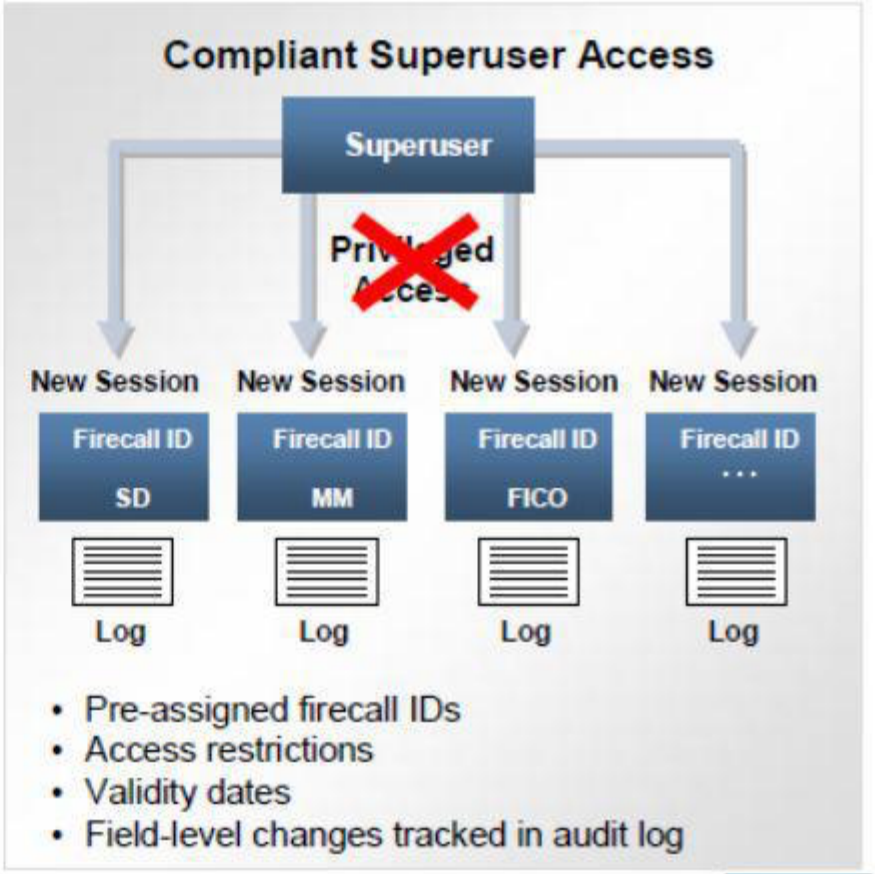


- Logging On creates a new SAP session as if the FF ID had logged on.



Firefighter





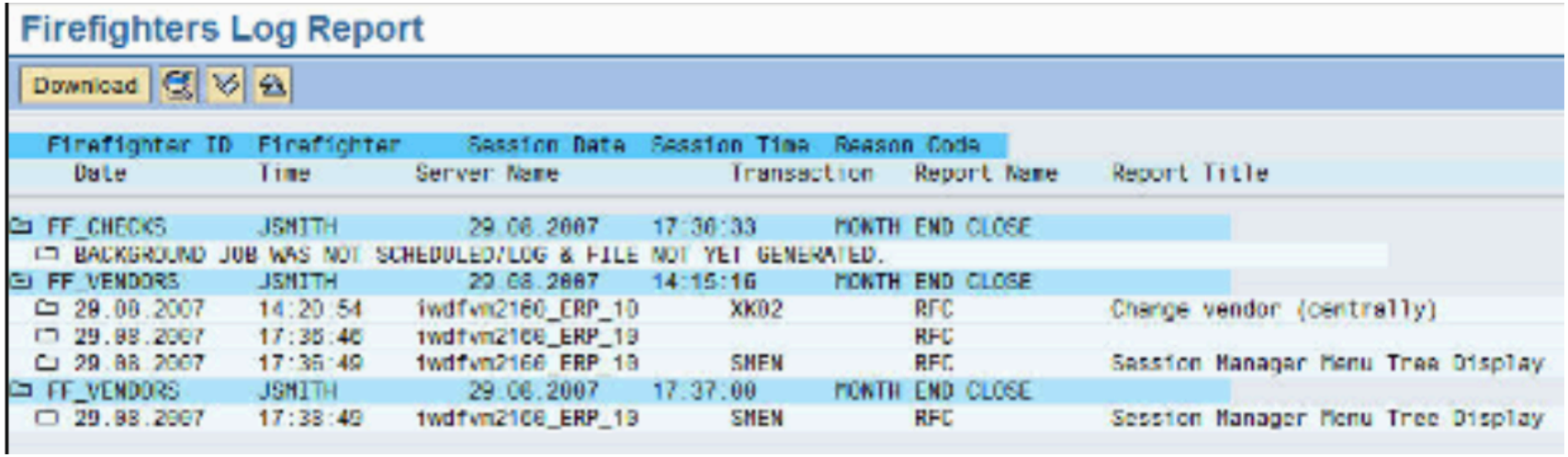
THE BEST-RUN BUSINESSES RUN SAP™

Firefighter / Emergency User

- 'Best' Practices
  - Documented FF / Emergency User Concept
  - 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'



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

GRC – Governance, Risk & Compliance

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

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

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

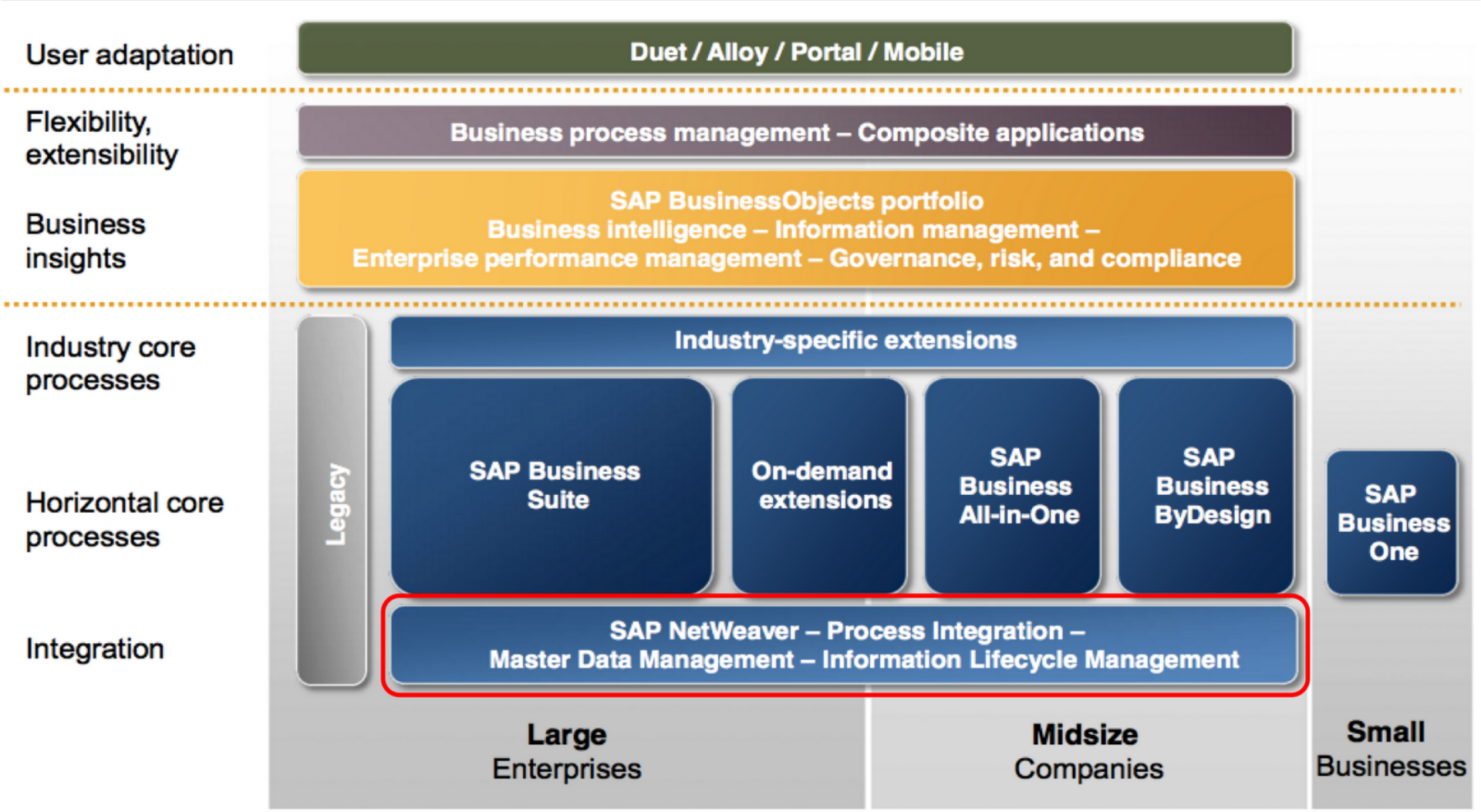
GRC: Governance, Risk & Compliance

Key Benefits

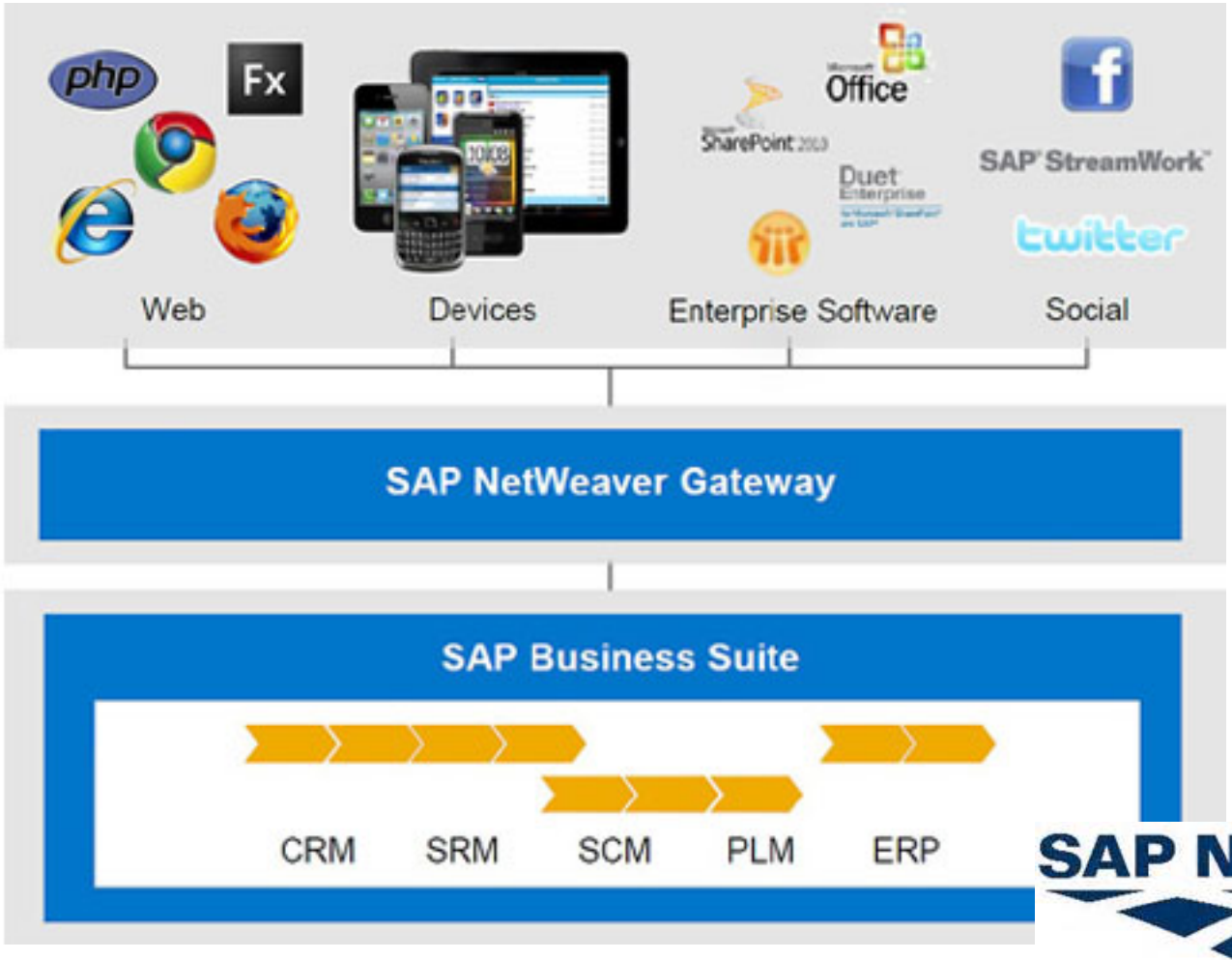
- Real-time analysis of SOD and SAT violations
- Possible automation of compliance requirements (SOX, FDA, etc.)
- Transparency of risks – align with strategic priorities and business objectives
- Proactive monitoring (centralized risk indicator framework)
- SAP integration makes implementation, maintenance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

Other SAP Solutions - Security

SAP: Not Just ECC/ERP



SAP: Business Suite



SAP CRM

CRM: Customer Relationship Management

Solution: managing all phases of customer interaction cycle

Security: Different paradigms vs. traditional SAP components (e.g. ECC, BI)

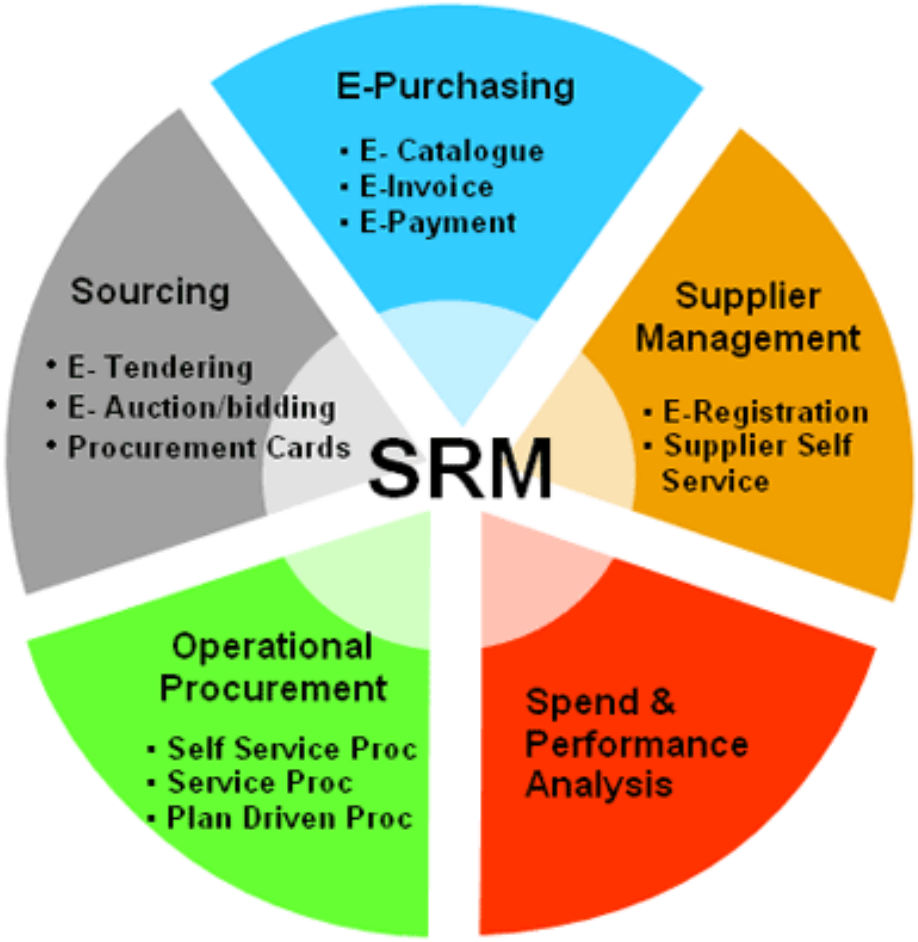
- WebClient UI links vs. traditional transactions (Internet apps)
- Role assignment by:
  - Directly via CRM User Master
  - Indirectly: User assigned a Position, Positions assigned business role
- CRM Territory Mgmt hierarchy (territory attributes further restrict access to customers and /or material)
- Use of multi-tier security restrictions

SAP SRM

SRM: Supplier Relationship Management

Solution:

- Automate / simplify Procure-to-Pay processes
- Strengthen supplier relationships



SAP SRM

SRM: Supplier Relationship Management

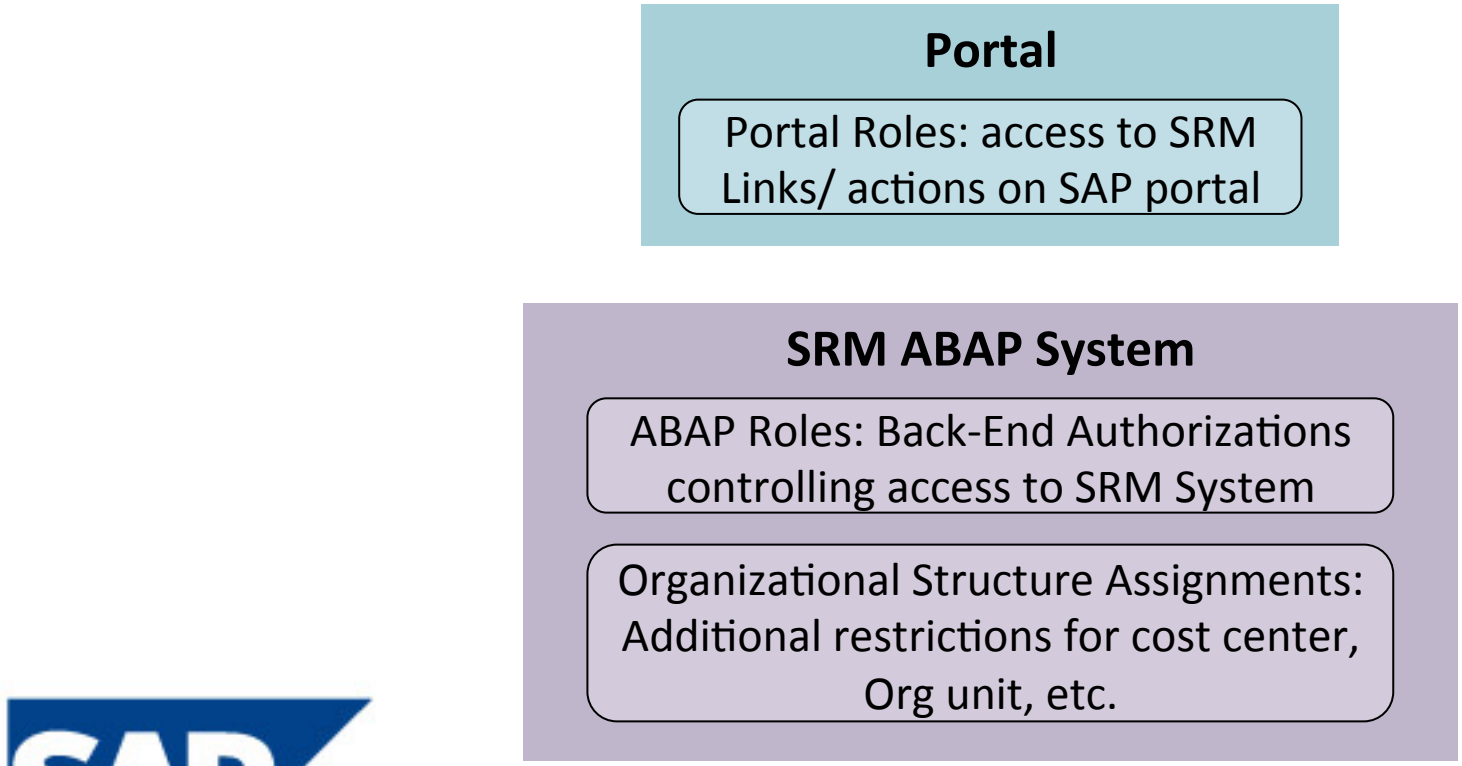
Security: Enterprise Buyer security options

- ABAP Security Roles
- SAP NetWeaver Portal Security Roles
- Organizational Structure and Attributes

Note: The 3 security layers / components must be tightly aligned and integrated to streamline the model

SAP: SRM Security Integration

Note: The 3 security layers / components must be tightly aligned and integrated to streamline the model



SAP® SRM

SAP BI

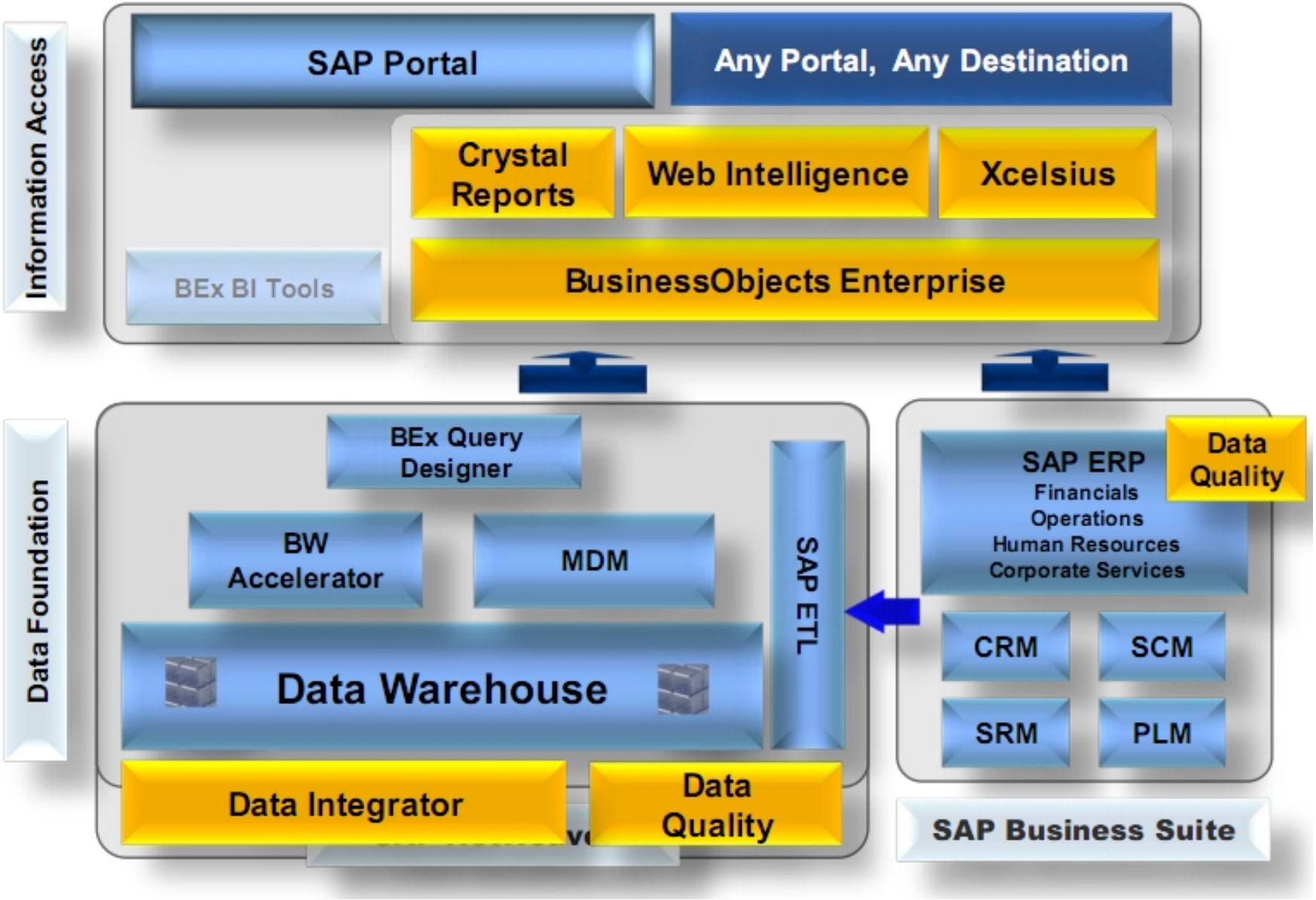
BW/BI: Business Warehouse / Business Intelligence

Solution:

- Business information for decision making
- BW – the information extractor, transform and consolidate (info-cubes) and one access tool
- BO – Business Objects: another information access tool

SAP Business Information Warehouse (SAP BW)

SAP BW Architecture



SAP BI Security

Security: is not transaction based

- Secure BW data objects:
  - Operational Data Store (typically the core data dump from process, transactions)
  - Info Cube
  - Info Source
- More detailed Security by data dimension (e.g. organizational object like company, plant, etc.)

SAP Business Information Warehouse
(SAP BW)

GRC & Other SAP Module Security Overview

- GRC
  - What are the GRC modules
  - What does 1-2 of the module do – reason for being
  - Benefit of GRC

- Pick another SAP Module and ..
  - Declare what the module does (why does SAP market it)
  - How Security id administered in this module vs. ECC

Assignment Questions

- **Did other people understand the specifics of this chapter?**

- I thought it was key (and very understandable) that these newer applications and tools would strive to link IT risks with Business Risks (what we are learning in other courses should be the case with every company). However, I would certainly love to see how all of this actually works, or at least a real-world examples? Maybe something from your experience on how to apply this.

- *How can we achieve good balance between automated control and manual controls?* When do you draw the line on automation?

- How can we implement balance scorecard over SAP GRC?

- Usually policy is rarely changed, how to define the life cycle of a policy?

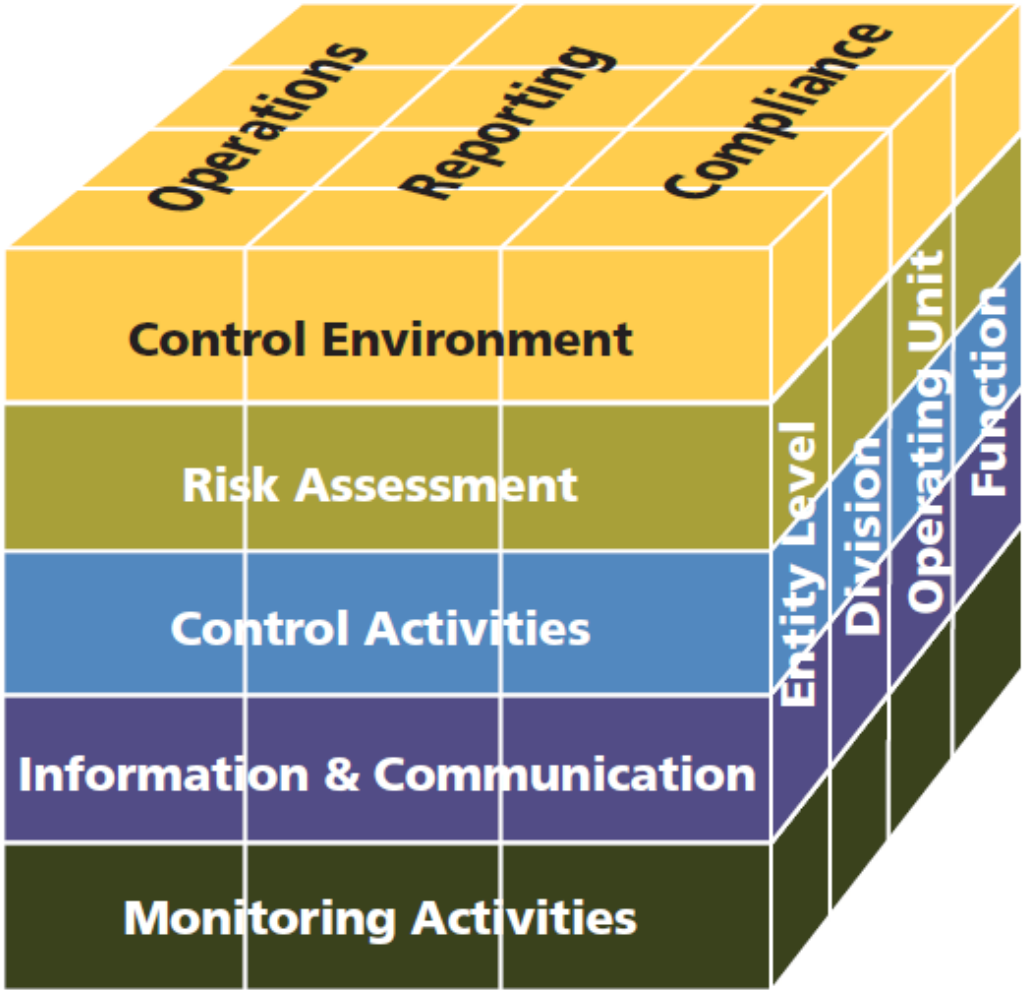
Assignment Questions

- Do you think it would be beneficial to hire an external expert in SAP to configure the settings, or configure the settings internally?
  Does an company always need all four integrated elements to strengthen ICS?

Break Time

Risk / Control Matrix
Final Exercise

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

Risk / Control Matrix: Final Exercise

- Agenda
  - Prior Class *(April 6)*: Part 1 (Identify Risks)
  - Prior Class *(April 13)*: Part 2, 3 (Identify Controls, Link Controls to Risks)
  - This Class *(April 20)*: Part 4 (Complete Control Definitions)
  - Future Class *(April 27)*: Part 5, 6 (Control Process / Audit Details; Personal Questions)
  - *Due April 30 11:59 PM:* Assignment Submission

Risk / Control Matrix: Final Exercise

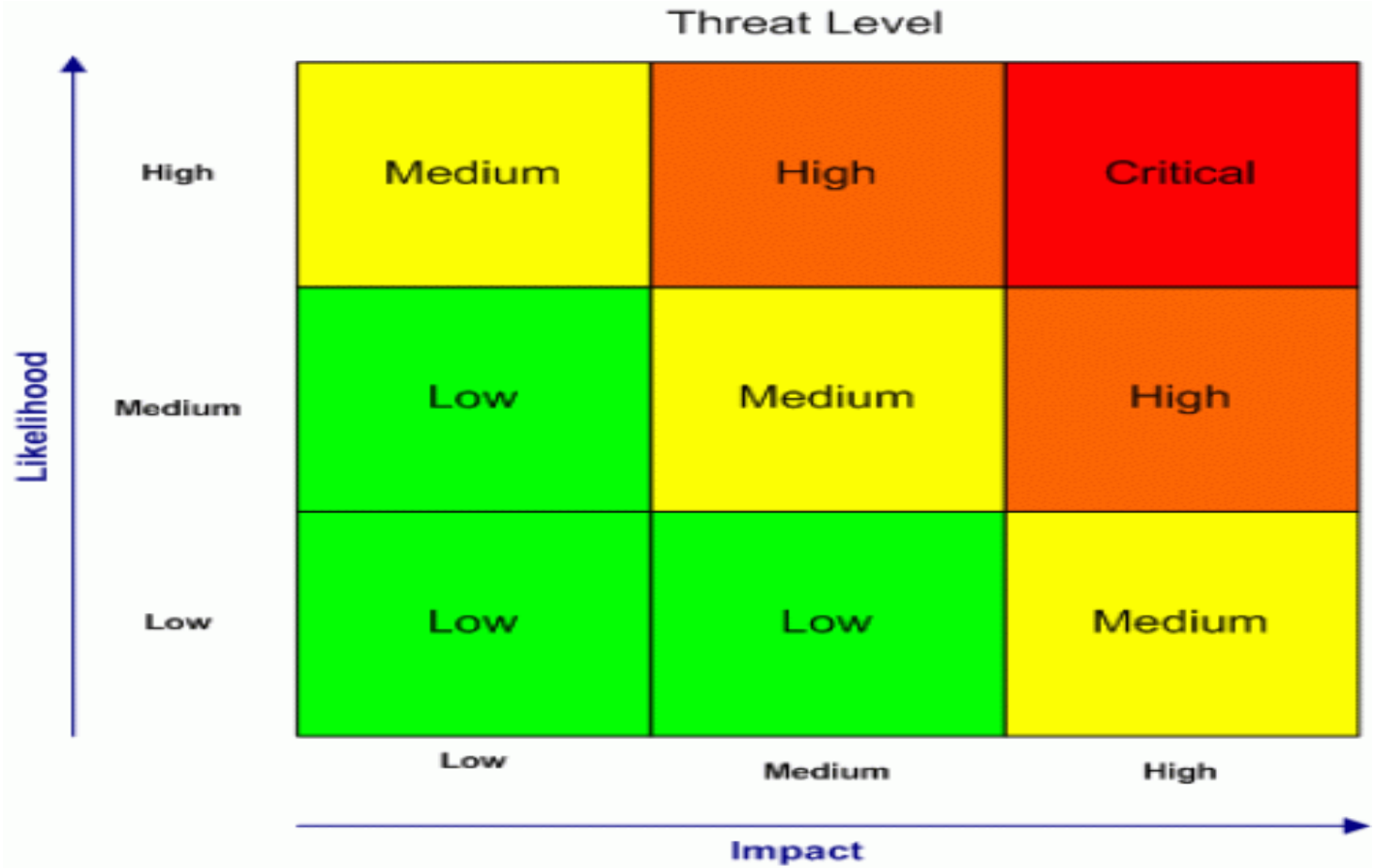
Part 4: Augment key controls information for the Order to Cash (OTC) process at GBI

- Tab: Part 2 – GBI Controls
- Control Description (Columns F -> I) Mark each using taxonomy provided
  - Control Owner (Title): Choose **one** title from Appendix 1 or define appropriate missing title
- Financial Statement Assertions (Columns J -> O) Mark with **X**
- Risk Assessment of control (Columns P -> S)
- Financial Statement Impact (Columns T -> AI) Mark statements impacted with **x**

Extra Slides

Risk Assessment

Extra Slides



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 a other exercises.

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 / 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)