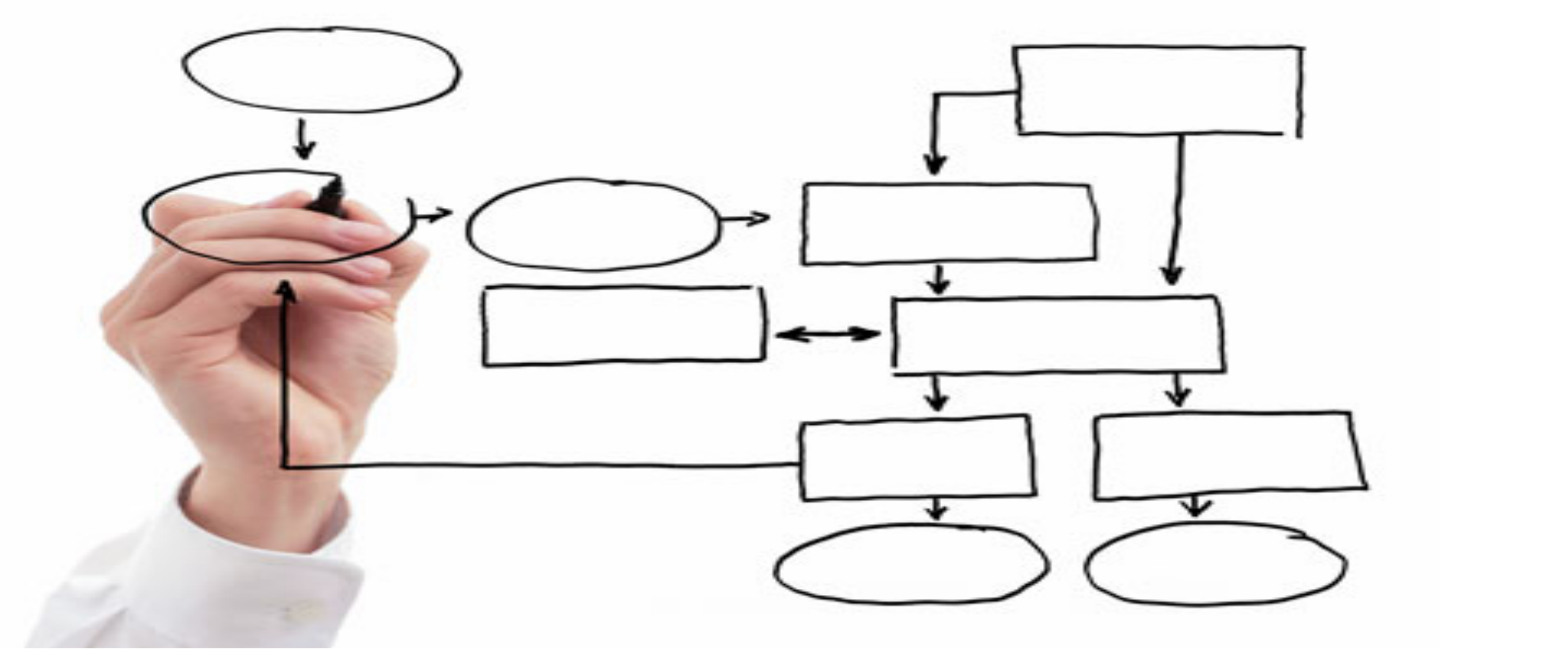


MIS 5121: Business Process, ERP Systems & Controls

Week 9: *Guest Lecture – Implementing, Auditing, and Securing SAP's Next Generation Applications*

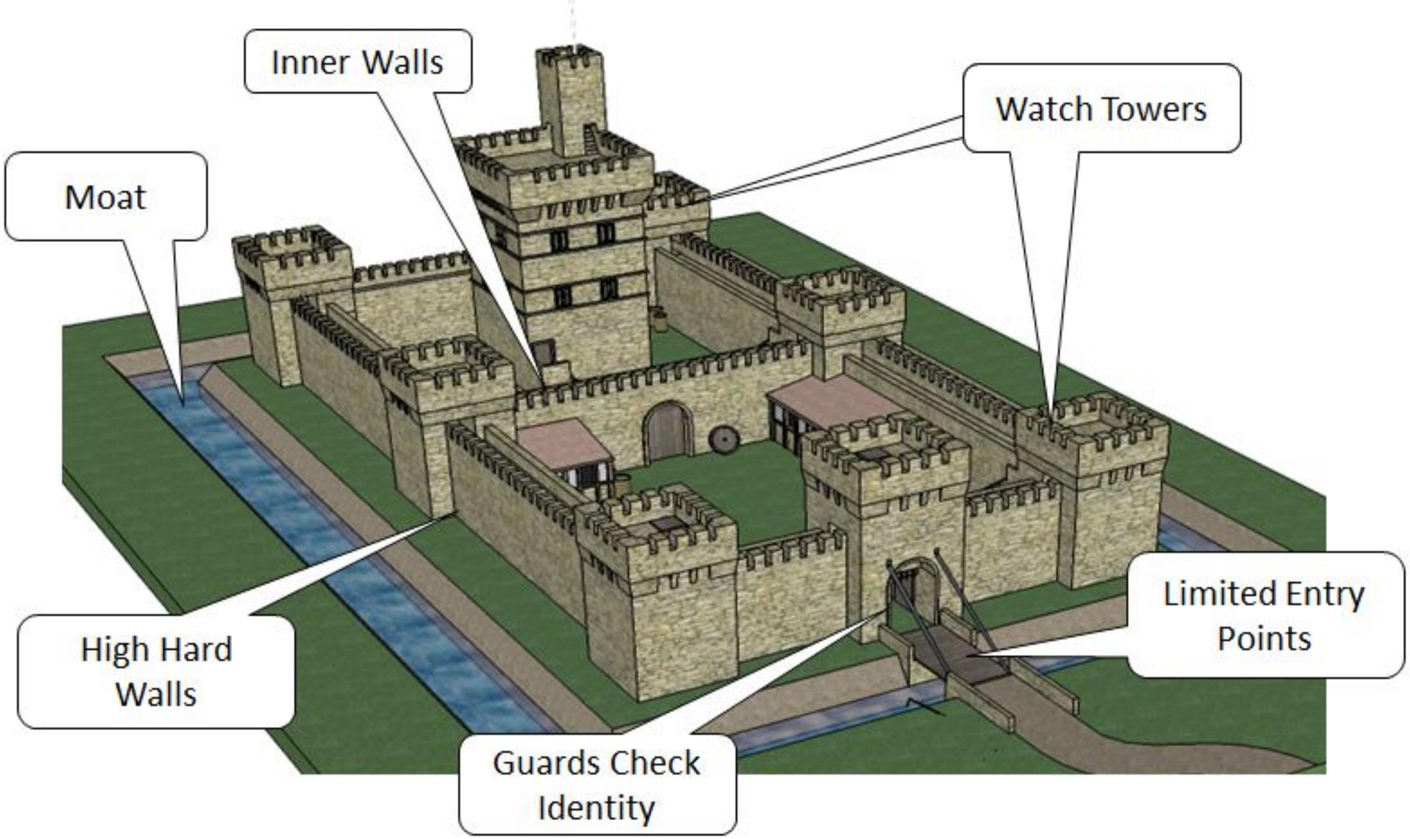
Steven Yannelli

Sr. Manager, Global SAP Security

CSL Behring

FOX | MIS
Management Information Systems

Guarding the Crown Jewels

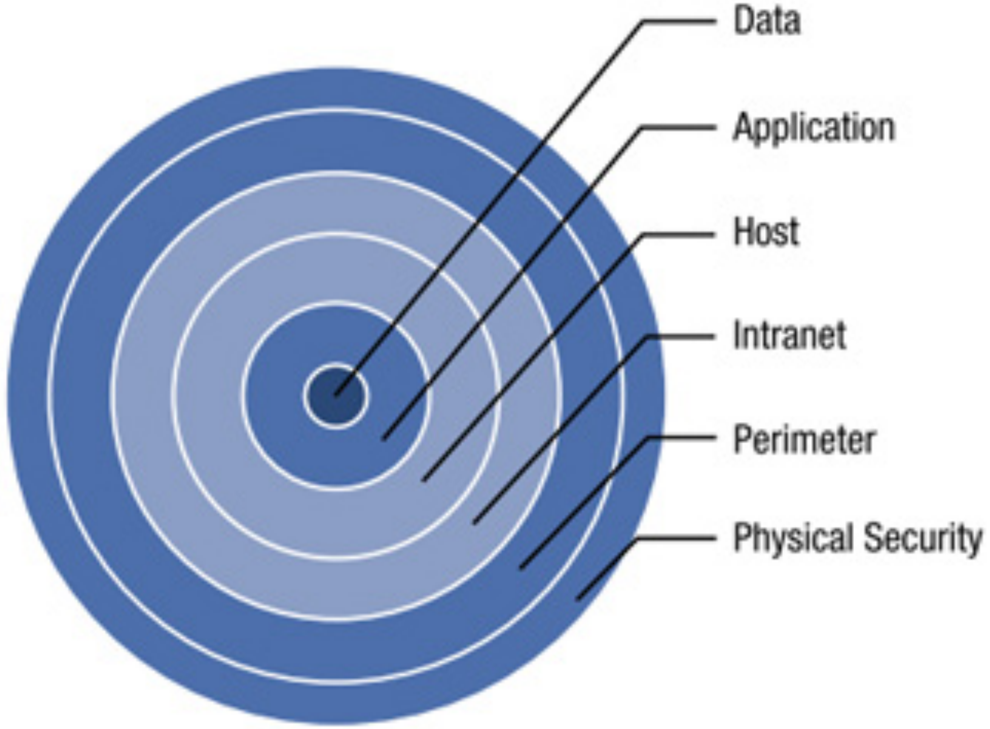


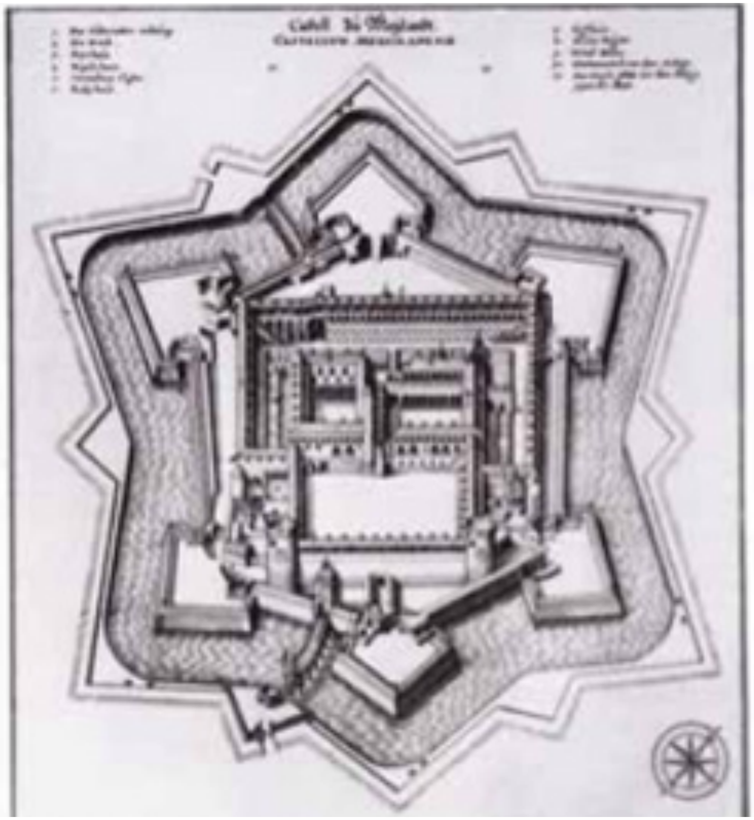
How do the concepts of protecting a castle relate to securing information?

Why did castles become obsolete?

“Defense in Depth”

Protective Layers Improve Security





Why Secure SAP?

External Threats:

- Hackers
- Nation State Actors
- Criminals

Internal Threats:

- Opportunistic or disgruntled employees
- Third party contactors

What are we Protecting?

Examples include:

- Credit card numbers
- Bank account routing and account numbers
- Personal health information
- Personal information (SSN, National ID, Passport numbers, etc…)
- Intellectual Property

Which of these elements is most valuable if sold on the open market?

Security & Internal Controls

Preventing or Detecting Fraud

Regulatory Compliance

Reduction of Risk

Preventing Accidents

Threat Map in Today's Environment

Impacts Actors	Financial Theft / Fraud	Intellectual Property Theft	Business Disruption	Destruction of Plant and Operations	Reputation Damage	Threats to Privacy (Patients, Suppliers, Employees)	Regulatory
Organized Criminals	🟦	🟦	🟨	🟦	🟨	🟧	🟦
Hactivists	🟦	🟦	🟨	🟦	🟨	🟧	🟦
Nation States	🟦	🟧	🟨	🟦	🟨	🟧	🟨
Insiders	🟧	🟧	🟨	🟦	🟨	🟧	🟨
Third Parties	🟦	🟧	🟨	🟦	🟨	🟧	🟦
Skilled Individual Hackers	🟦	🟨	🟨	🟦	🟨	🟧	🟩

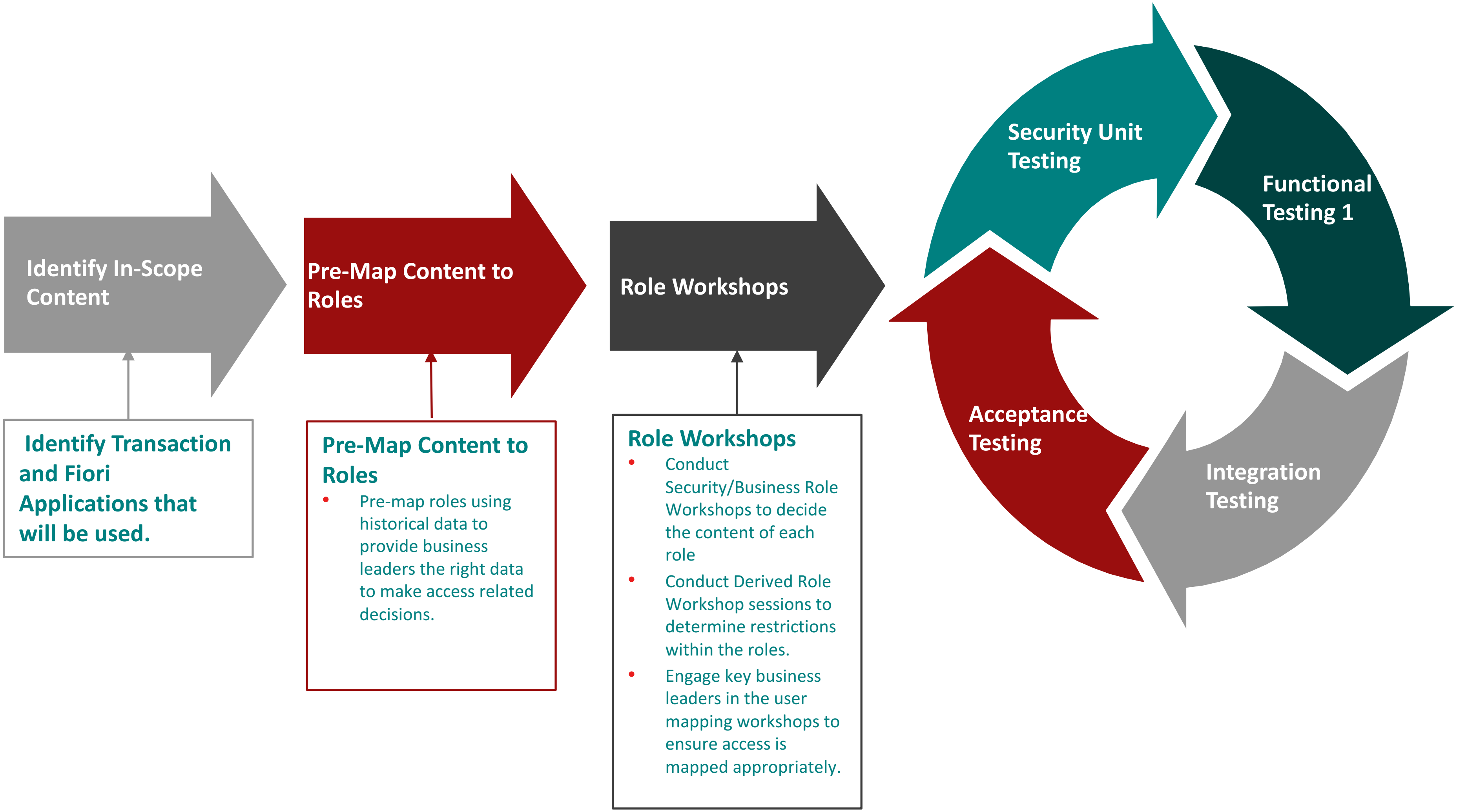
- 🟥 Almost Certain
  Greater than one event per year
- 🟧 Likely
  One event every 1 – 5 years
- 🟨 Possible
  One event every 6 – 10 years
- 🟦 Unlikely
  One event every 11 – 50 years
- 🟩 Highly Unlikely
  Less than one event 50 years

Designing and Building SAP Roles

SAP Security Implementation Steps

1. Determine what is in scope for the project
2. Determine the design approach.
    1. Task Based Roles
    2. Job Based Roles
3. Map the content to roles.
4. Determine requirements for more granular restrictions within each transaction/role.
5. Test, test, test.
6. Figure out who gets access to which role.
7. Cutover & Go-Live!

SAP Security Development and Testing Process



Identify In-Scope Content

Pre-Map Content to Roles

Role Workshops

Security Unit Testing

Functional Testing 1

Integration Testing

Acceptance Testing

Identify Transaction and Fiori Applications that will be used.

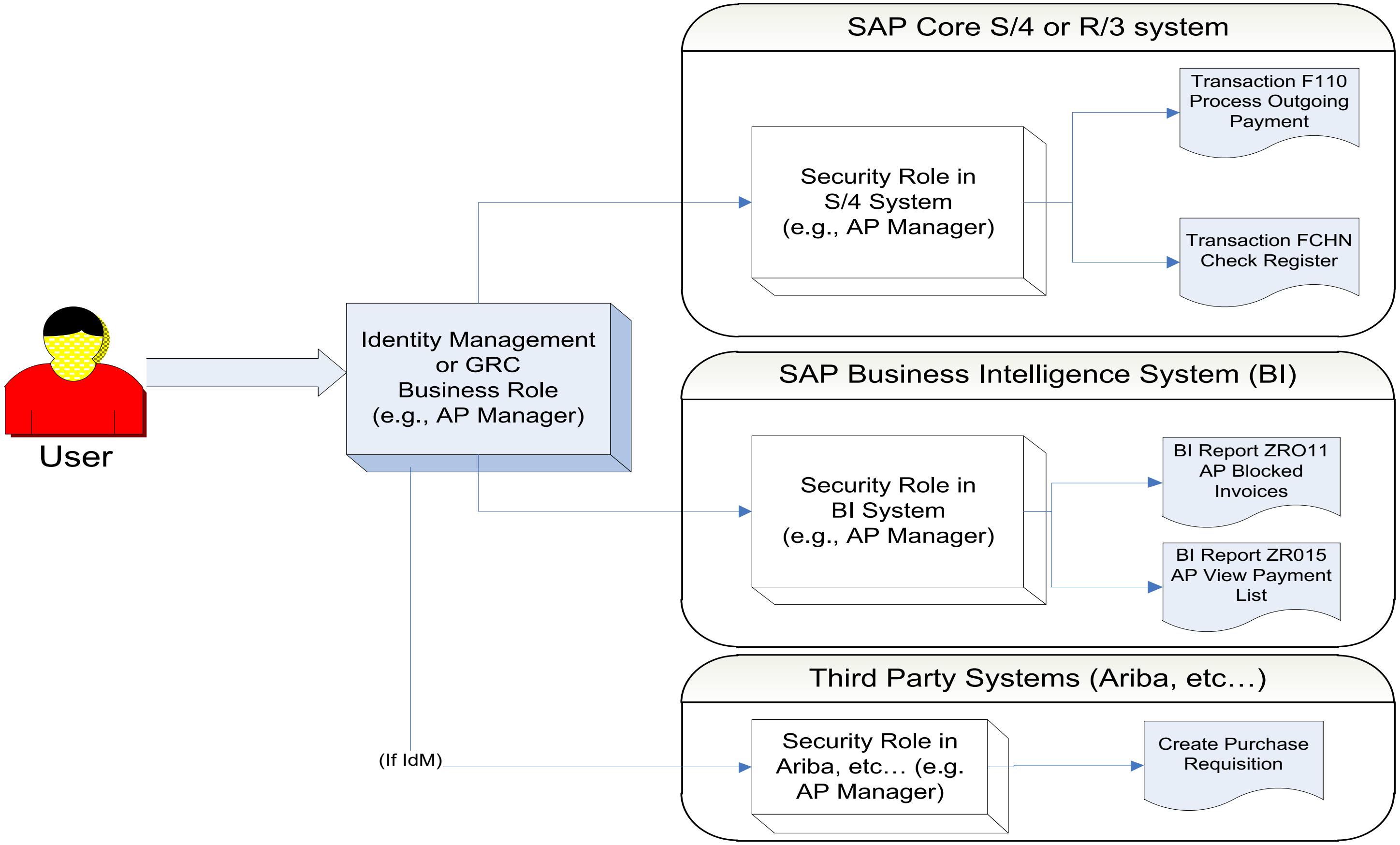
Pre-Map Content to Roles

- Pre-map roles using historical data to provide business leaders the right data to make access related decisions.

Role Workshops

- Conduct Security/Business Role Workshops to decide the content of each role
- Conduct Derived Role Workshop sessions to determine restrictions within the roles.
- Engage key business leaders in the user mapping workshops to ensure access is mapped appropriately.

Business Role Concepts


SAP Core S/4 or R/3 system
Transaction F110 Process Outgoing Payment
Security Role in S/4 System (e.g., AP Manager)
Transaction FCHN Check Register
User
Identity Management or GRC Business Role (e.g., AP Manager)
SAP Business Intelligence System (BI)
BI Report ZRO11 AP Blocked Invoices
Security Role in BI System (e.g., AP Manager)
BI Report ZR015 AP View Payment List
Third Party Systems (Ariba, etc…)
(If IdM)
Security Role in Ariba, etc… (e.g. AP Manager)
Create Purchase Requisition

Terminology:

Security Role - logical grouping of transactions performed in SAP within a discrete functional area.

Business Role - collection of security roles. A Business role is a package of security roles that provide access. Business roles loosely relate to positions within the company.

Questions?

Auditing SAP

Typical Audit Engagement

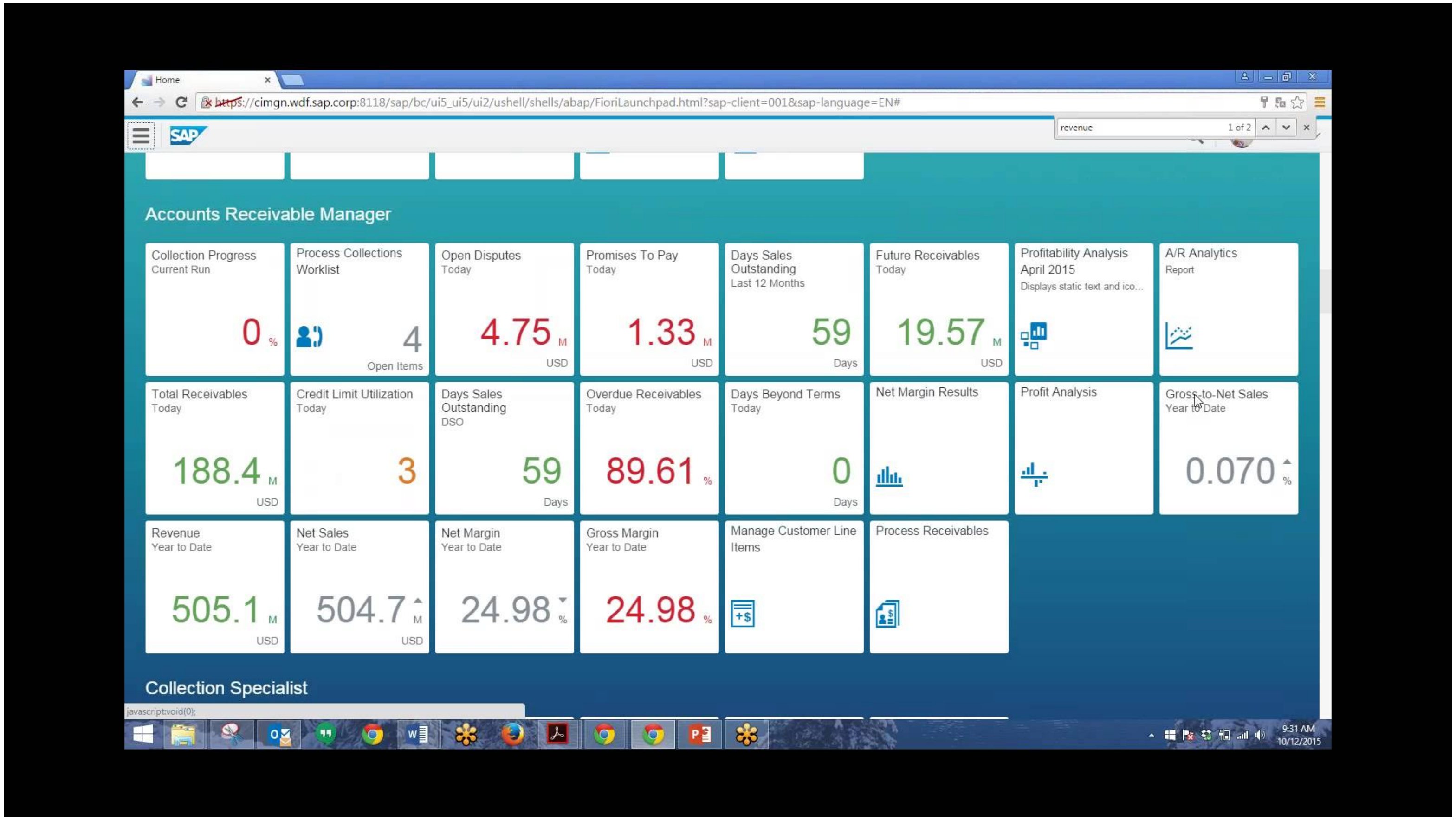
1. Determine scope.
2. Initial Meetings – Tactical Approach & Last Period Results
3. Information is requested and exchanged.
4. Auditor assessment of information
5. Develop findings, observations, and improvements
6. Findings/observations/improvements are remediated and documented.

Types of Auditors & Responsibilities

- **External Auditors** can tell you what is wrong, but not how to fix it. In U.S. publicly held companies, external audit companies are not permitted to sell services to help you fix problems.
  - Why? Companies were using audit findings as a way to sell services.
- **Internal Auditors** have resources to help identify issues internally, prepare you for audit, highlight risk, and help develop controls. Internal auditors cannot be control owners.
- **Consultants and employees** implement and manage controls.

Questions?

The Future of SAP Technology



https://cimgn.wdf.sap.corp:8118/sap/bc/ui5_ui5/ui2/ushell/shells/abap/FioriLaunchpad.html?sap-client=001&sap-language=EN#

Accounts Receivable Manager

Collection Progress
Current Run
0 %

Process Collections Worklist
4
Open Items

Open Disputes
Today
4.75 M
USD

Promises To Pay
Today
1.33 M
USD

Days Sales Outstanding
Last 12 Months
59
Days

Future Receivables
Today
19.57 M
USD

Profitability Analysis April 2015
Displays static text and ico...

A/R Analytics
Report

Total Receivables
Today
188.4 M
USD

Credit Limit Utilization
Today
3

Days Sales Outstanding
DSO
59
Days

Overdue Receivables
Today
89.61 %

Days Beyond Terms
Today
0
Days

Net Margin Results

Profit Analysis

Gross-to-Net Sales
Year to Date
0.070 %

Revenue
Year to Date
505.1 M
USD

Net Sales
Year to Date
504.7 M
USD

Net Margin
Year to Date
24.98 %

Gross Margin
Year to Date
24.98 %

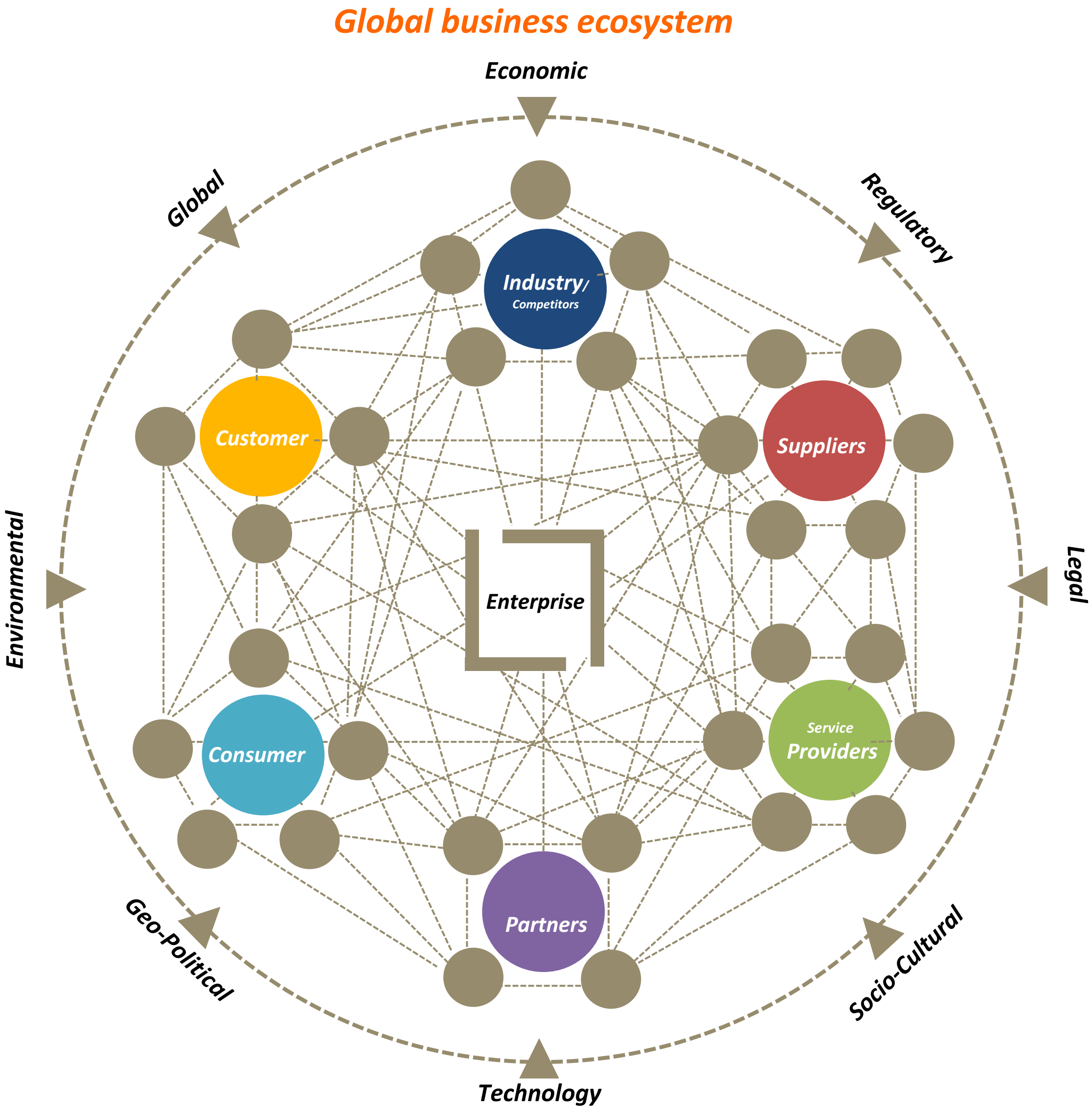
Manage Customer Line Items

Process Receivables

Collection Specialist

javascript:void(0);

Traditional Security Models are Changing Due to Globalization



Information Technology Market Forces

1. Shift to the cloud
2. Increased demand for mobility –

- Think about your own web browsing experience over the past 5-10 years. People expect the same experience at work.

3. "Big Data" – Companies are trying to gain intel from larger datasets faster (SAP HANA)

4. Adoption and User Experience are market differentiators.

5. Business lines no longer need the IT department to make buying decisions - driving innovation.

SAP’s Response to Market Demands

- **SAP HANA** – in memory database that drastically speeds up the way information is stored and accessed.
- **SAP Fiori** – presents a much better look & feel and mobile friendly environment. Prevents people from having to go to various internal SAP systems to do a process task.
- Emergence of “buy versus build” with cloud applications.

Questions?

Demo

SAP® Fiori

[Business Overview: https://www.youtube.com/watch?v=Io9HfoVkGVU](https://www.youtube.com/watch?v=Io9HfoVkGVU)

[Navigation: https://www.youtube.com/watch?v=yey4hUSR7Og](https://www.youtube.com/watch?v=yey4hUSR7Og)

New & Exciting Opportunities/Jobs

- Identity and Access Management
  - Single Sign-On providing automation in logging in
  - Automates setting up, managing, and disabling people’s accounts in systems.
  - Automates requesting additional access
  - Integrates your Human Resources system with your IT processes for improved security & governance.
- Cyber Security field growing substantially
  - Many companies are creating security tools in today’s market.

Career Paths in Audit/Consulting

- Audit/Consulting firm (PwC, Deloitte, KPMG, Ernst & Young are “Big 4”)
  1. Associate/Experienced Associate – Junior level, responsible for working on components of an audit.
  2. Senior Associate – developed expertise in specific areas, serves as knowledge expert and manages larger portions of an overall audit. More heavily client facing.
  3. Manager/Sr. Manager – responsible for managing audit teams, involved in SOW/contracts, responsible for quality and accuracy of overall work product.
  4. Director - Senior leadership of the firm, may serve as leads on larger clients. These are typically employed positions.
  5. Partner/Principal – Executive leadership of the firm, may serve as leads on larger clients. These individuals establish relationships with senior client leadership. These individuals buy into a share of the company and it’s profits.

Tips for Auditors

1. Become an expert in something
2. Be professional, courteous and tactful
3. Listen – be open to other control methods
4. Ask a lot of questions
5. Establish a working relationship with your co-workers and clients

Career Paths in Information Security

- Industry
  1. Analyst – Responsible for monitoring systems, completing requests, performing tasks for projects.
  2. Senior Analyst – further developed expertise, leads project components.
  3. Manager/Sr. Manager – Leads larger scale security projects/initiatives.
  4. Director or Information Security Officer – This level is sometimes the highest level of security professional in many small to mi-size companies.
  5. Chief Information Security Officer or VP, Information Security – Executive security leader within the company, responsible for all matters related to Information Security