



Coca-Cola Enterprises Inc.


**Case Study: Implementing Security Access Controls
Through Role-Based Security**

Robert Greenberg, Kyleen Wissell, Kim Kever

Coca-Cola Enterprises Inc. 

Today's Agenda

- Introductions
- Session Objectives
- Who is CCE?
- Background
- What are the Objectives?
- CCE Vision
- Project Approach / Case Study
- Challenges and Lessons Learned
- Q&A

Coca-Cola Enterprises Inc. 

Session Objectives

1. What is Role-Based Access Control (RBAC)?
2. What are some of the pros/cons of implementing RBAC?
3. What should you know (and need to know) before considering an RBAC project?
4. How can your company's appetite for governance determine the effectiveness of security access controls?
5. What are the business drivers for an enterprise Identity Management solution? And what are the components for an effective implementation?
6. What is the relationship and synergy between the business and IT that is necessary for developing a role-based security framework of users and permissions?
7. What methodologies, tools, information and resources are required to execute satisfactory outcomes?
8. If the potential benefits of role-based access governance are substantial, are also the challenges to achieving it equal?
9. What are some Lessons Learned by those having embarked on the road to Role-Based Security Access?


3

Coca-Cola Enterprises Inc. 

Who is CCE?

Coca-Cola Enterprises

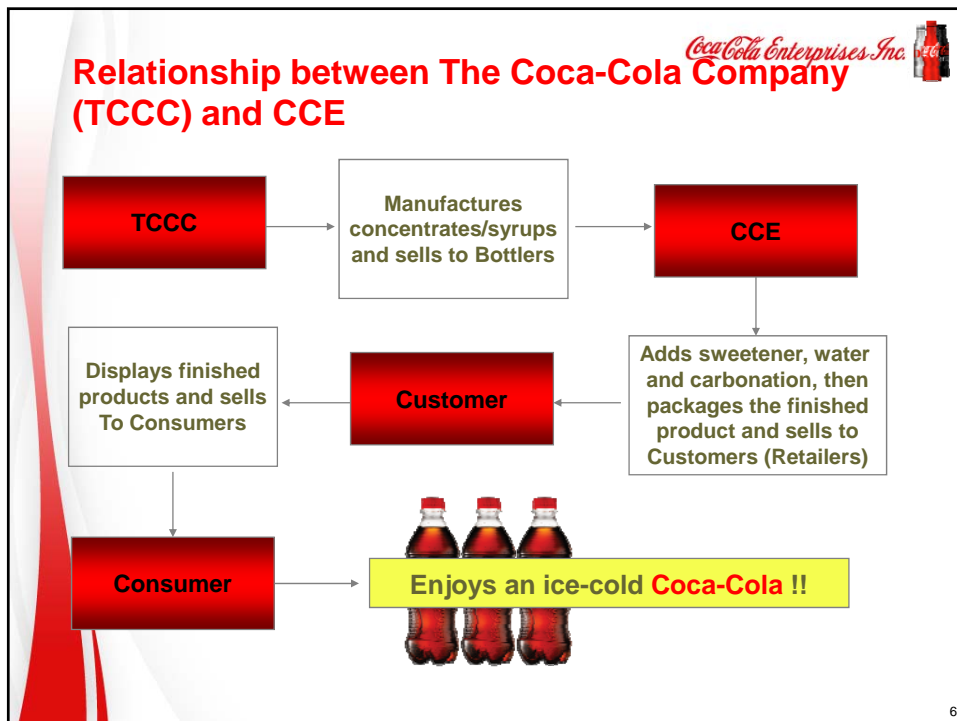
4



Coca-Cola Enterprises Inc.

- World's largest non-alcoholic bottler
- Represents 16% of The Coca-Cola Company's global volume
- Two billion physical cases sold in 2009
- Equivalent to 41 billion bottles and cans
- \$22 billion in annual revenues
- 74,000 Employees
- 444 Facilities in North America and Europe

5






Background




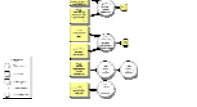
Security Access Controls (SAC) Program at CCE

7

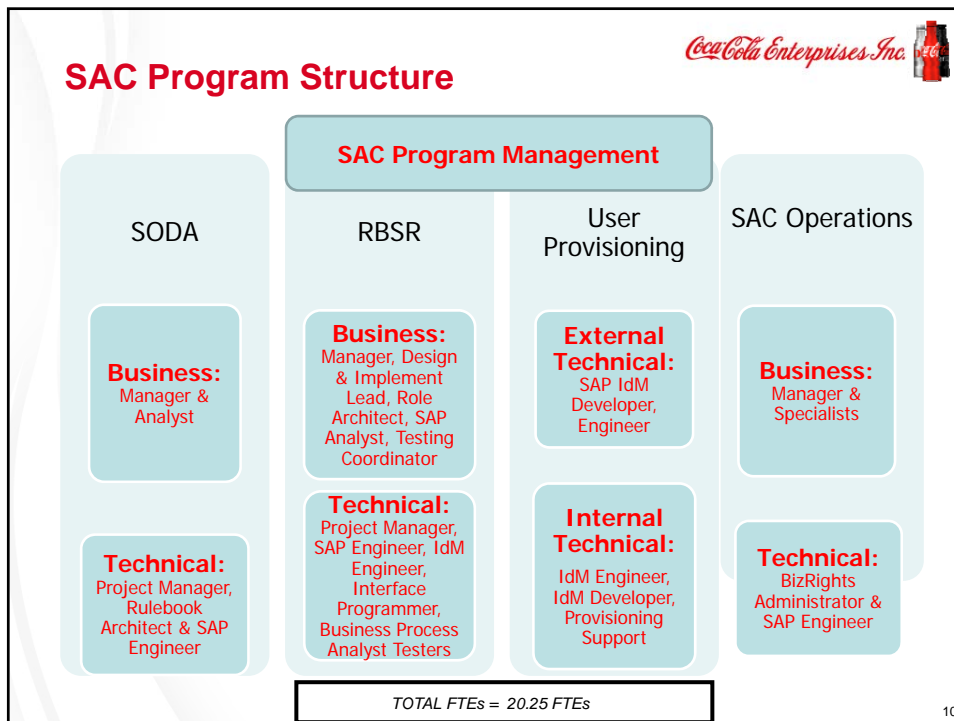
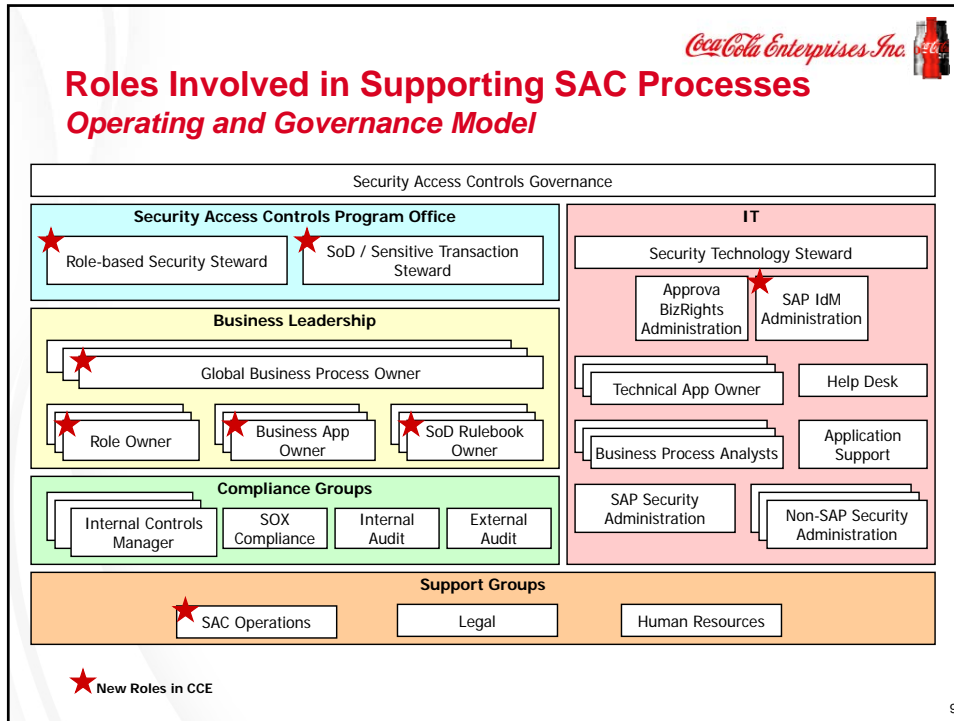



Security Access Controls (SAC) Program

Global, multi-year effort at CCE, challenging

<p>SODA Project</p>	<p>The Segregation of Duties Analysis (SODA) focuses on identifying risks, documenting SoD and sensitive transaction rules, implementing rules to prevent and detect (SoD) violations, and implementing processes to sustain rulebooks.</p>	<p>Robert Greenberg</p>	
<p>RBSR Project</p>	<p>The Role-based Security Redesign (RBSR) focuses on designing and implementing role-based security for key business processes, applications, and associated users. Leveraging HR master data for automatically assigning access to employees.</p>	<p>Kyleen Wissell</p>	
<p>UP Project</p>	<p>User Provisioning (UP) focuses on implementing a new provisioning tool and associated workflow processes to provided role-based security to users, free of segregation of duties violations.</p>	<p>Security Operations</p>	
<p>SAC Program Mgmt</p>	<p>The Program-level activities focus on managing the overall program, navigating around issues and driving critical problem resolution, measuring progress and success, and leading cross-project activities.</p>	<p>Kimberly Keever</p>	

8






What are the Objectives?

Security Access Controls (SAC) Program at CCE

11




Security Access Controls Executive Summary

What is it?	Why is it Important?	What is the Impact?
<ul style="list-style-type: none"> A process which enables an authority to control access to areas and resources in a given physical facility or computer-based information system* Should be a business-led initiative (it's a business problem, not an IT problem) Designed to strategically enhance capabilities for access controls (people, processes, technologies, internal controls) Effectively and efficiently manage security access to applications, data, and networks 	<ul style="list-style-type: none"> It is a key component of managing a company's risk Managing access in a large company is a challenge Hundreds of applications, computer systems, and networks Tens of thousands of employees, contractors, third-parties, and other users Regulatory requirements have increased scrutiny in this area -- can affect auditor opinions on financial statements 	<ul style="list-style-type: none"> It touches every part of the organization that uses computer systems It can affect: <ul style="list-style-type: none"> What a person's job function is How easy it is perform that job How quickly one can receive access to systems It changes the processes associated with: <ul style="list-style-type: none"> Requesting and approving access Performing and testing internal controls

* Source: http://en.wikipedia.org/wiki/Access_control


12

Coca-Cola Enterprises Inc. 

What are the Drivers for Security Access Control Improvements?

Reduce Information Security Risk	Improve Regulatory Compliance	Reduce Security Overhead	Improve User Satisfaction
<ul style="list-style-type: none">Risks are inherent any time access is provided, but can be reduced by implementing better security access controls, such as knowing who has access to what, how access is relevant to a particular job, and how user access rights are removed	<ul style="list-style-type: none">Regulatory requirements have increased (example, Sarbanes-Oxley legislation in the United States), and this has added complexity and increased external scrutiny of access management processesProvide reasonable assurance that data is protected against unauthorized use, modification, disclosure, fraud, loss, or impairment	<ul style="list-style-type: none">Managing security for a large number of applications and systems and for a large user base that changes frequently is tedious, complex to administer, and difficult to monitor and validate	<ul style="list-style-type: none">Appropriate access should be provided in a timely manner so people can perform their jobs and be productive sooner

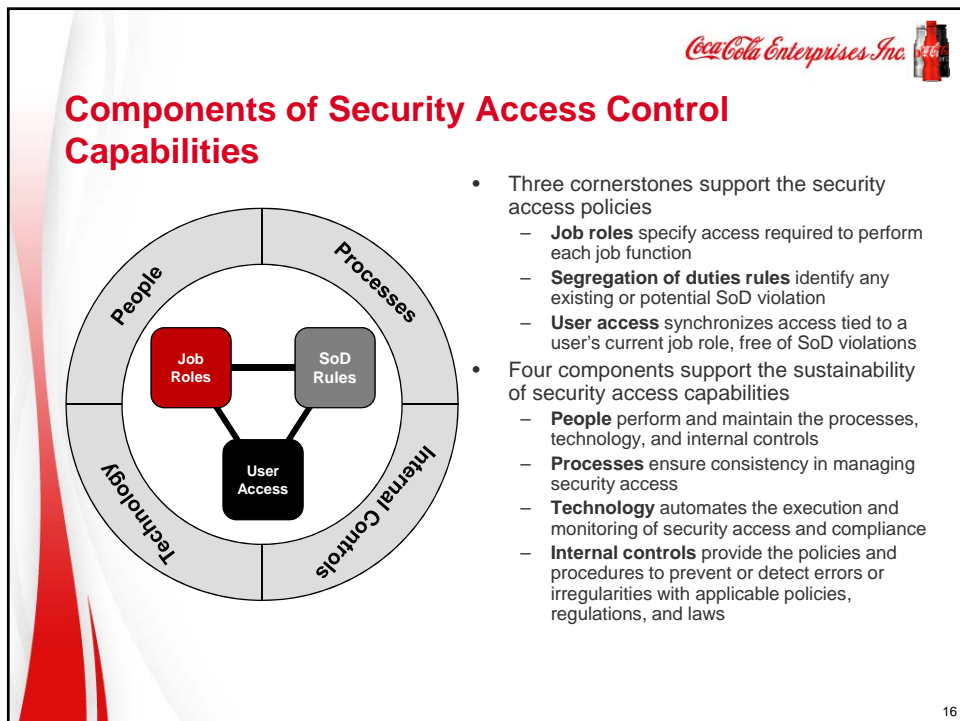
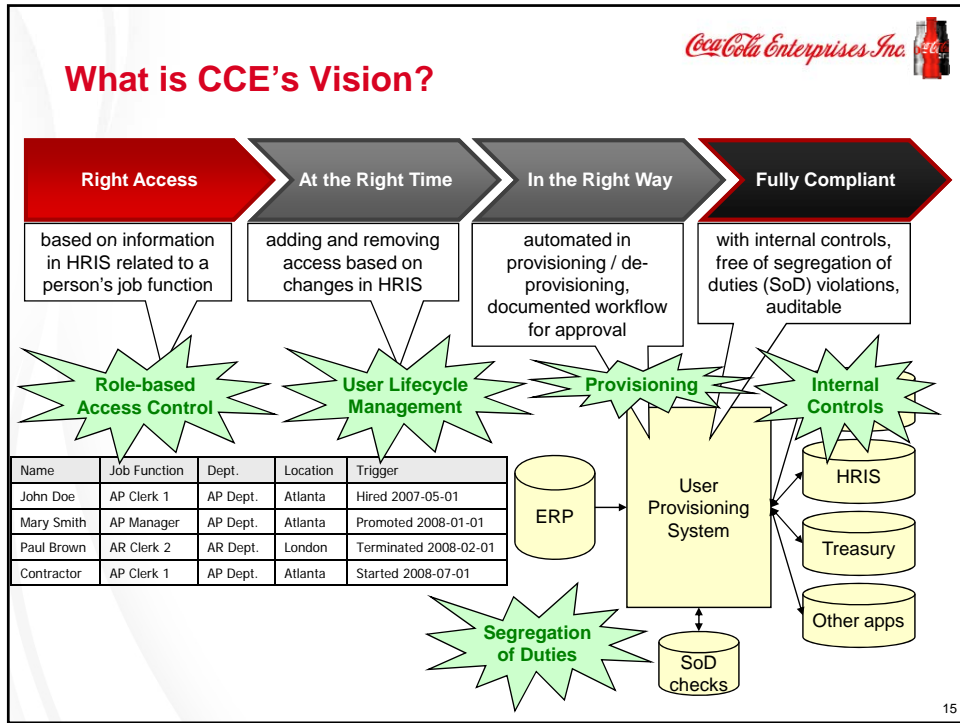
13

Coca-Cola Enterprises Inc. 

What is CCE's Vision?

Key Program Components

14

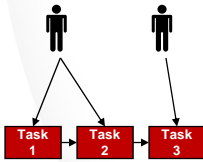




Segregation of Duties

What is it?

A primary internal control intended to prevent or decrease the risk of errors or fraud by assigning conflicting duties to different personnel



Examples

- The same person should not be able to both "create sales orders" and "issue credit memos"
 - Risk: A person could create a sales order, generating fraudulent revenue, and then reverse the revenue in a subsequent period by issuing a credit memo
- The same person should not be able to both create vendor master records and process accounts payable payments
 - Risk: A person could create a fictitious vendor and generate fraudulent payments to the vendor

Types of controls

- Preventive controls**
- Design job roles with SoD in mind and verify no issues before finalizing roles
 - Before granting additional access to a user, evaluate the request for additional access against existing user access to determine if conflicts would arise
- Detective controls**
- Check SoD rules against existing access provided to users

Separation of duties is viewed as a critical component of an organization's internal control structure whose primary objective is to reduce the opportunity for fraud and the occurrence of errors

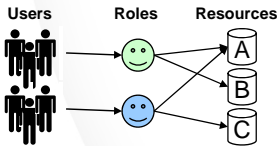
17



Role-based Access Control (RBAC)

What is it?

- Granting access privileges to a user based upon the work that they do (using a risk based approach)
- Access rights are given to roles, and users are assigned to roles – all users of a certain role are given the same access



Example

- A user is granted an "AP Clerk" role and gets all of the access required to perform the AP Clerk function


Connection to SoD

- A role should be checked against the segregation of duties (SoD) rules to verify there is no conflict for the role
 - Redesign the role to eliminate the conflict, or
 - Establish a compensating control if there is a business reason for the same person to do both

Less effective ways

- In an ad-hoc fashion, granted on an as-needed when-needed basis
 - Rarely revoked
 - Everyone becomes unique over time
- Through cloning - give Joe the same rights as Jane
 - Could give someone extra access not needed
- These role management practices result in security breaches, increased complexity in managing privilege assignments, and inability to verify and enforce compliance

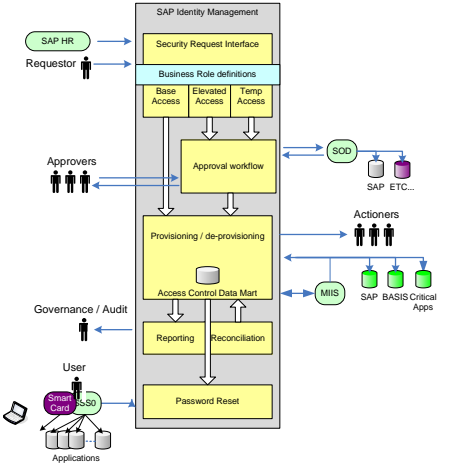
18

Coca-Cola Enterprises Inc. 

User Provisioning and User Lifecycle Management


**User Provisioning:
What is it?**

- Providing system access to users
- When combined with role-based security, users are assigned roles and access is provisioned with the access rights for that role
- Ideally, additional access can be provisioned only if temporary, approved, and does not cause SoD conflicts with existing access



The diagram illustrates the SAP Identity Management architecture. It shows a central 'SAP Identity Management' box containing several components: 'Security Request Interface', 'Business Role definitions' (with sub-categories: Base Access, Elevated Access, Temp Access), 'Approval workflow', 'Provisioning / de-provisioning', 'Access Control Data Mart', 'Reporting', 'Reconciliation', and 'Password Reset'. External entities interact with these components: 'Requestor' (SAP HR) sends requests to the Security Request Interface; 'Approvers' interact with the Approval workflow; 'Actioners' (SAP, etc.) execute provisioning/de-provisioning; 'Governance / Audit' and 'User' interact with Reporting and Reconciliation; and 'Applications' (Smart Cards, etc.) interact with Password Reset. The Access Control Data Mart is linked to 'MIS' and 'SAP BASIS Critical Apps'.


19

Coca-Cola Enterprises Inc. 

Segregation of Duties

Project Approach

20


Coca-Cola Enterprises Inc. 

People Involved in SA and SOD Rule Design

Resources needed to define, validate and execute ongoing approach

Position	Responsibilities
Rulebook Owners (RBOs)	<ul style="list-style-type: none"> Accountable for one or more rulebooks. These individuals are responsible for defining, executing and enforcing the process of reviewing violations, designing remediation plans and maintaining rules. RBOs are responsible for reviewing access requests that have failed the preventive SoD/SA rule checks, to determine whether to approve or reject the request.
Business Process & Sub-Process SMEs	<ul style="list-style-type: none"> Understands the relationship between the key business processes across the company and the day-to-day functions of users within the identified in-scope business area. These individuals should be capable of decomposing business processes, understand risks associated with these identified processes (e.g., segregation of duties). Often delegated responsibility to lead violation analysis / remediation plan development.
Business Process Analysts (BPAs) – IT	<ul style="list-style-type: none"> Understands key security features in the identified applications, including the relationship between platform and internal security features with business processes Serves as a liaison between the Rulebook Owner(s) and SAP Security Engineer to facilitate rule design, violation remediation and/or mitigation activities. Performs / responsible for Functional Unit Testing of technical rule designs.
Information Security Engineers - IT	<ul style="list-style-type: none"> Demonstrates understanding of security functions and administration for specific applications and security related policies and procedures. Responsible for completing the Technical Design of rules, based on the approved Business Requirements Assists in understanding the best way to address rule violations.
SAC Operations Team	<ul style="list-style-type: none"> Understands the rule development approach / methodology and the supporting technologies related to the rule design process.

21


Coca-Cola Enterprises Inc. 

Guiding Principles for Rulebook Development

Guiding Principle	How to Apply It
Include the appropriate level of management and subject matter experts in determining what are the right rules needed by the business	<ul style="list-style-type: none"> Perform a risk analysis to identify the risk considerations important to the business. Determine the appropriate rules that address management and auditor concerns. Secure management buy-in and support to ensure sustainability.
Document rule decisions, requirements and rationale. Obtain appropriate consensus from the business including sign-off.	<ul style="list-style-type: none"> Capture rule requirements in business terms, using business speak. Document the rule descriptions and control objectives in the requirements. Describe requirements in sufficient detail, so the business requirements can be translated into technical rule designs for the transactions involved. Ask the business to sign-off on final business requirements documents.
User access to sensitive transactions, as well as IT systems in general, should be in line with their job responsibilities	<ul style="list-style-type: none"> Clearly define and document roles & responsibilities of each position. Ensure that roles are designed to match assigned job responsibilities. Verify access is not too broad and that it does not contain SoD conflicts. Document which transactions are sensitive and should be monitored.

Compliance Advisor / SME Guidance and Input

22

Coca-Cola Enterprises Inc. 

Mitigating Risks related to SoD Conflicts

Under the concept of SoD, business critical duties can be categorized into four types of functions: **Authorization**, **Custody**, **Record keeping**, and **Reconciliation**. In a perfect system, no one individual should handle more than one type of function

If a single individual can carry out and conceal errors and/or irregularities in the course of performing their day-to-day activities, they have been assigned incompatible job responsibilities. When job responsibilities cannot be separated, compensating controls should be identified and put in place.

There are several control mechanisms that can help to enforce the segregation of duties:

- Audit trails
- Reconciliation
- Exception reports
- Transaction logs
- Supervisory review
- Independent reviews

23

Coca-Cola Enterprises Inc. 

Project Approach – Case Study for Role Base Security Redesign

Analyze, Design, Build, Test, Deploy, Sustain

24



People Involved in Role Design

Resources needed to define, validate and execute ongoing approach

Position	Responsibilities
Business Process Owners (BPOs)	<ul style="list-style-type: none"> Accountable for one or more business processes. These individuals often serve as the project sponsors on the business side and supervise Business and Application SME's Often BPOs become Business Role owners with business contacts who access various applications, manage roles for business area and is able to evaluate impacts of changes on the existing design
Business Process & Sub-Process SMEs	<ul style="list-style-type: none"> Understands the relationship between the key business processes across the company and the day-to-day functions of users within the identified in-scope business area These individuals should be capable of decomposing business processes, understand risks associated with these identified processes (e.g., segregation of duties) Often delegated responsibility for role engineering, membership and role definition certification from the business role owner
Business Process Analysts (BPAs) – IT	<ul style="list-style-type: none"> Understands key security features in the identified applications, including the relationship between platform and internal security features with business processes Provides application-specific functional, data, and / or access control expertise and knowledge to Role Engineering Analysts / Role Governance Team during application role engineering and maintenance processes Often delegated responsibility for role engineering, membership and role definition certification
Information Security Engineers - IT	<ul style="list-style-type: none"> Demonstrates understanding of security functions and administration for specific applications and security related policies and procedures.
Role Based Security Team	<ul style="list-style-type: none"> Understands Role Based methodology and the supporting technologies related to completing a role engineering project plus understanding of business processes

25



RBSR Redesign Case Study – Order to Cash North America

- Involved Thirty-five Role Owners and subject-matter experts and sixteen Business Process Analysts (BPAs) engaged to design Business Roles
- Nine business sub-processes were analyzed for both US and Canada
- Total of 20 Business Roles determined and designed
- Impacted 500 employees and 350 non-employees
- Steps performed included:
 - Documenting business activities
 - Linking applications to activities
 - Reviewing and linking detailed privileges to applications
 - Identifying Candidate Business Roles
 - Documenting thousands of detailed authorizations into a single framework for each Business Role

Business Sub-Process	Functional Role
AR Cash Receipts	AR Cash Receipts Performer AR Cash Receipts Approver AR Support Performer
Customer Marketing Agreement Accounting	CMA Performer CMA Specialist CMA Approver
Collections / Customer Service	Collections Performer Collections Approver
Credit Management	Credit Management Performer
Dispute Management	Dispute Management Performer
Customer Master Data	Master Data Performer Master Data Approver
Pricing	Pricing Performer Pricing Full Service Performer Pricing Approver
Route Settlement	Route Settlement Performer US Route Settlement Performer CAN Route Settlement Approver
Equipment Settlement	EC Settlement Performer EC Settlement Approver
TOTALS	20 functional roles

26



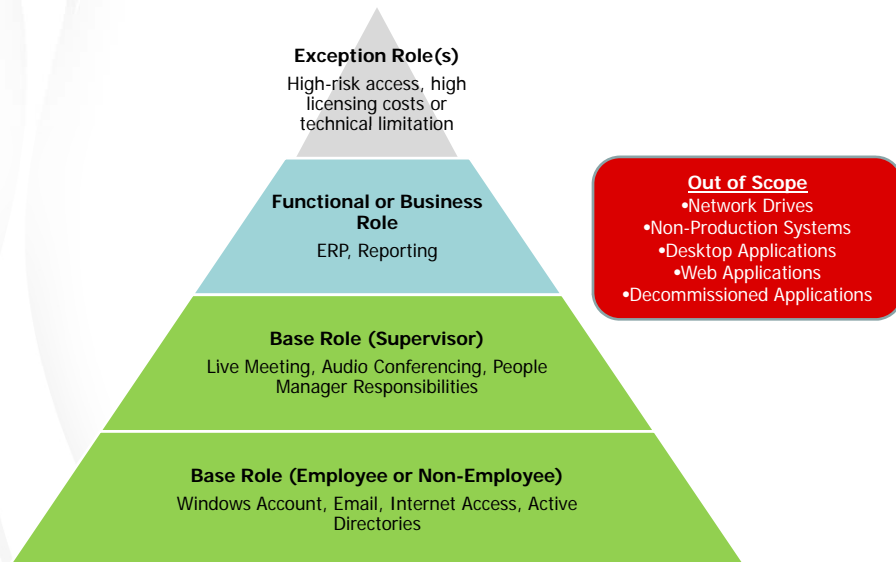
RBSR Scope & Approach

1. Business roles for OTC access to over 80 production applications for internal and outsource users
2. Team leveraged SODA work to-date and determined repeatable procedures for role design, build, test and deploy and designed processes for sustainable operations
3. Approach emphasized role reuse considering OTC Europe to follow
 - Execute validation of existing roles to promote continental reuse
 - 'Layer' access requirements into RBSR framework as a series of role change management projects
4. Early identification of HR clean up tasks, segregation of duties conflicts and sensitive access concerns will determine whether you can stay on track with your timeline
5. Determine how your users will get access for applications determined out of scope

27



Layering System Access



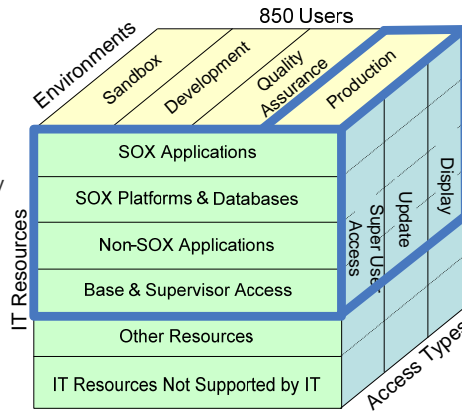
28

RBSR – Application Scoping Exercise

Landscape Analysis:

Area highlighted in **blue** represent RBSR scope:


1. Supporting IT Resources
 - SOX applications
 - SOX platforms & databases
 - Enterprise applications that satisfy evaluation criteria based upon usage
 - Base & Supervisor access
2. Production Environment
 - Address risk
 - Make progress
 - Achieve benefits
3. Types of Access
 - Display
 - Update
 - Super User



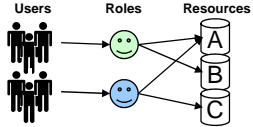
Risk-based Approach

Challenges

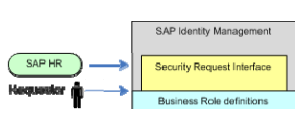
...and Lessons Learned

Coca-Cola Enterprises Inc. 

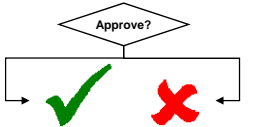
Challenges



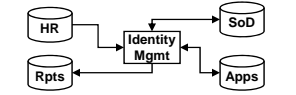
Standardizing and Minimizing Number of Roles
Each person thinking their job is unique and requires different access



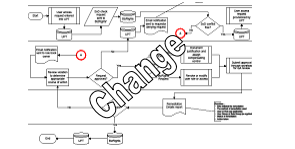
Leveraging HR Data
HR data maintained in a timely manner, kept accurate and consistent



Following New Processes
Managers and Owners following and maintaining processes, approving/rejecting requests and changes in a timely manner




Implementing and Supporting New Technologies
Integrated automated provisioning, workflow approvals, automated segregation of duties checking, and reporting seamlessly and reliable to be used for audit evidence



Sustaining Roles as Business Changes
The people, processes, and technologies to keep roles up-to-date

31

Coca-Cola Enterprises Inc. 


Key Takeaways

1. Executive Communication

- Steering Committee meets every 2 months to report on progress
- Reporting to Audit Committee quarterly promotes awareness
- SAC Program Manager attends IT Leadership monthly meetings to escalate issues
- Bi-weekly update meetings with Executive Sponsors

2. Involvement is important

- Identify and assign the right resources
- Engage and educate the business along the way
- Develop relationships with key IT team members
- Build critical capabilities and procedures
- Involve auditors and have regular checkpoints to review scope and approach



Lessons Learned

3. Evaluate Benefits

- Show how risk is reduced or mitigated
- Establish a SAC operations function for sustainability
- Evaluate customer satisfaction and expand tools and templates when necessary
- Focus on reducing risk and migrating higher numbers of users in lower risk areas to show progress

32



Q&A

33



Thank you

*Questions or comments concerning these materials
can be directed to...*

Robert Greenberg
770-200-8942
rgreenberg@cokecce.com

34