ISE Central Executive Forum and Awards
Nominee Showcase Presentation

June 9, 2010

Company Name:	TXU Energy
Project Name:	SAP "Roles Rebuild" Project
Presenter:	Chris Holm
Presenter Title:	Director – IT Risk, Security & Control

TXU Energy Company Overview

TXU Energy:

- Is the largest Retail Electric Provider (REP) in Texas ($6B)

- Has 2 million+ Residential and Business customers, supported by 5,000+ employees,

- Leads the TX electric market in innovative energy efficiency, community & customer service

Presentation Overview

- Overview / Challenges

- Goals of SAP "Roles Rebuild" project

- Project Plans & Methodology

- Results & Lessons Learned

- Q&A / Contact

Overview of Business Challenge

- Launched SAP business platform in Jan-May '09 for all customers; initial SAP application security Roles didn't work when applied at Go-Live

- 35%+ of all business & IT users were granted "excessively" broad access to perform job roles

- Security, Control & Audit issues resulted

"Roles Rebuild" Scope/Goals

- Scope: Every single SAP user at TXUE (3100+)
- Objectives:
  - Reduce access for 225+ job Roles to just what's needed for normal business (Ops, Sales, Support)
  - Review / define SoD data for incompatible duties for follow on work
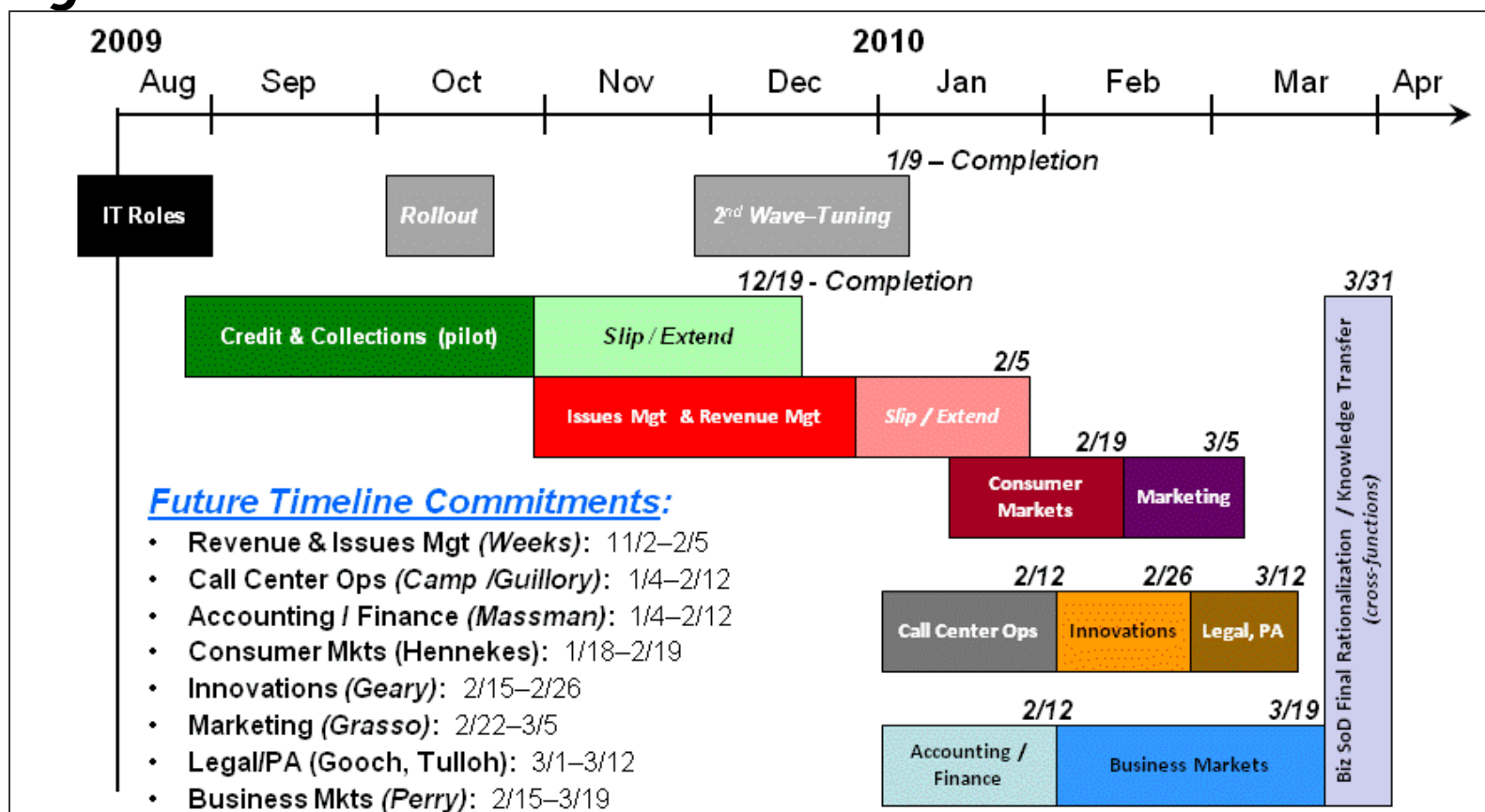 - Get it **ALL** done right by 3/31/2010

"Roles Rebuild" Challenges

- ~1 year since SAP Go-Lives....so users "used" to excessive access...didn't realize their power

- Feasibility of reducing sensitive access to Operational / Sales areas, potentially creating biz workflow problems

- Functional business priorities / projects distract Biz / IT teams from analysis, testing & coordination

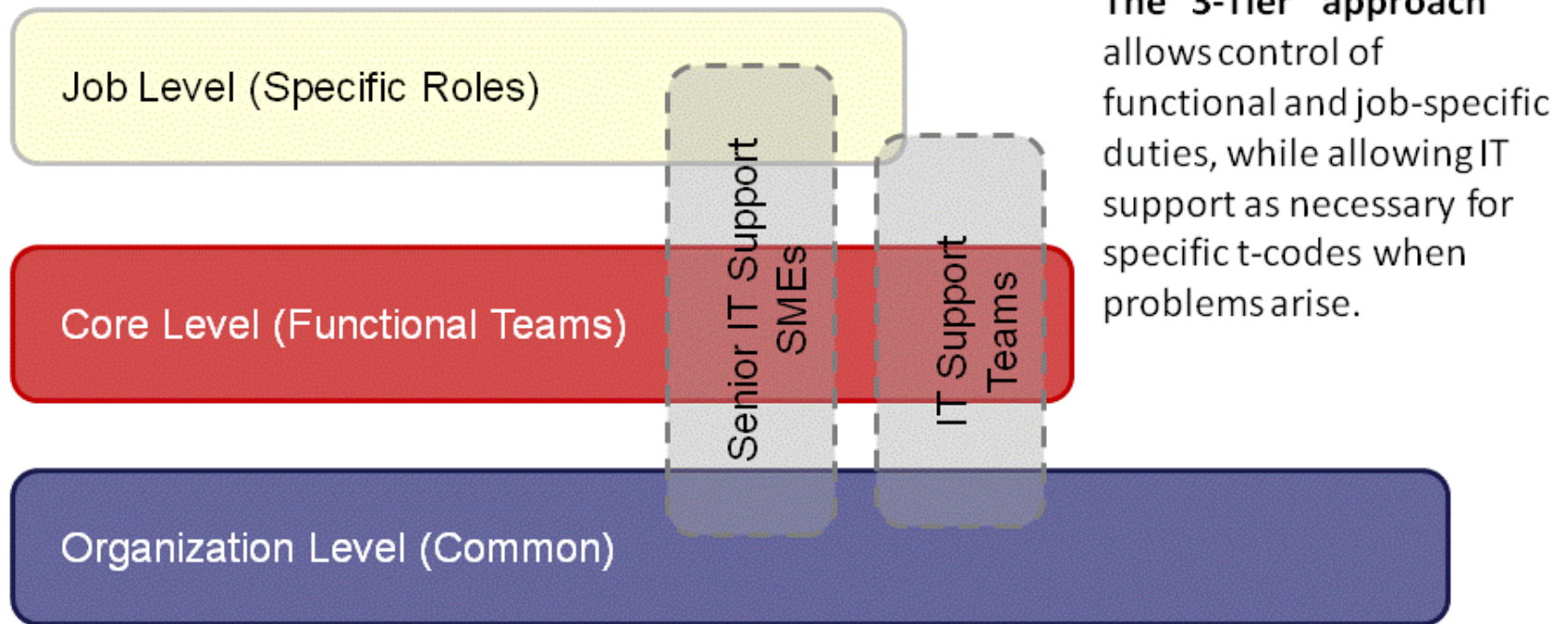- ...and significant Audit / Board attention

Project Plan as of 12/18/31

Role Rebuild Methodology

Job Level (Specific Roles)

Core Level (Functional Teams)

Organization Level (Common)

Senior IT Support SMEs

IT Support Teams

The "3-Tier" approach allows control of functional and job-specific duties, while allowing IT support as necessary for specific t-codes when problems arise.

Project Results

- Completed last Rebuild effort on 3/31 (exactly)

- 99.3% of users were in compliance with the new "1 user, 1 Role" policy as of 3/31

- Previous ~80 Roles grew to 230+ Roles, enhancing SoD

- Completed SoD review (using Approva BizRights)

- …and we just chartered the <u>SoD Remediation</u> program, anticipated to be completed Nov 2011

Lessons Learned/Best Practices

- Get joint Business-IT leadership accountability, otherwise effective speed is impossible

- "Goldilocks" pilot phases are invaluable

- SoD is impossible without basic RBAC

- Ensure expectations with Auditors are in synch

  (or somebody will be disappointed)

Thank you and Questions

- Questions?