Rethink Possible

Using Archer to Monitor Security Compliance at AT&T

Rebecca Finnin

Director, Chief Security Office

Agenda

- **Archer Overview**
  - *What is it and why would you use it?*
- **Security Governance, Risk and Compliance (GRC) at AT&T**
  - *Overview of department functions*
- **AT&T Multi-Year Archer Roadmap**
  - *Future State: Vision for Integrated Archer Solutions*
  - *Initial Deployment: Isolated Silos & Too Much Customization*
  - *Roadmap: Plan to move from Current to Future State*
- **Lessons Learned**
  - *If we had to do it over again – what could we do better?*

Archer Overview

Rethink Possible

Archer: What Is It?

- Archer is off the shelf software available from RSA division of EMC.
- The software is intended to 'provide the foundation for a best-in-class enterprise governance, risk and compliance program, by allowing you to automate, manage measure and report across your enterprise.'
- Archer software is billed as a flexible framework – i.e. you can modify it to meet your organizations specific requirements.
- In Archer Terminology the components of the FRAMEWORK are SOLUTIONS made up of APPLICATIONS. Standard SOLUTIONS include:
  - Policy Management
  - Risk Management
  - Compliance Management
  - Enterprise Management
  - Incident Management
  - Vendor Management
  - Threat Management
  - Business Continuity
  - Audit Management

Archer: Why Would You Use It?

- Archer provides a means to get compliance functions OUT of excel worksheets!!!!!
- It has all the benefits of web-based applications including:
  - Centralized, real-time reporting
  - Visual dashboards
  - Automated workflow and email notifications
  - Integrated view of controls, testing results, remediation plans, etc.

Security GRC at AT&T

Rethink Possible

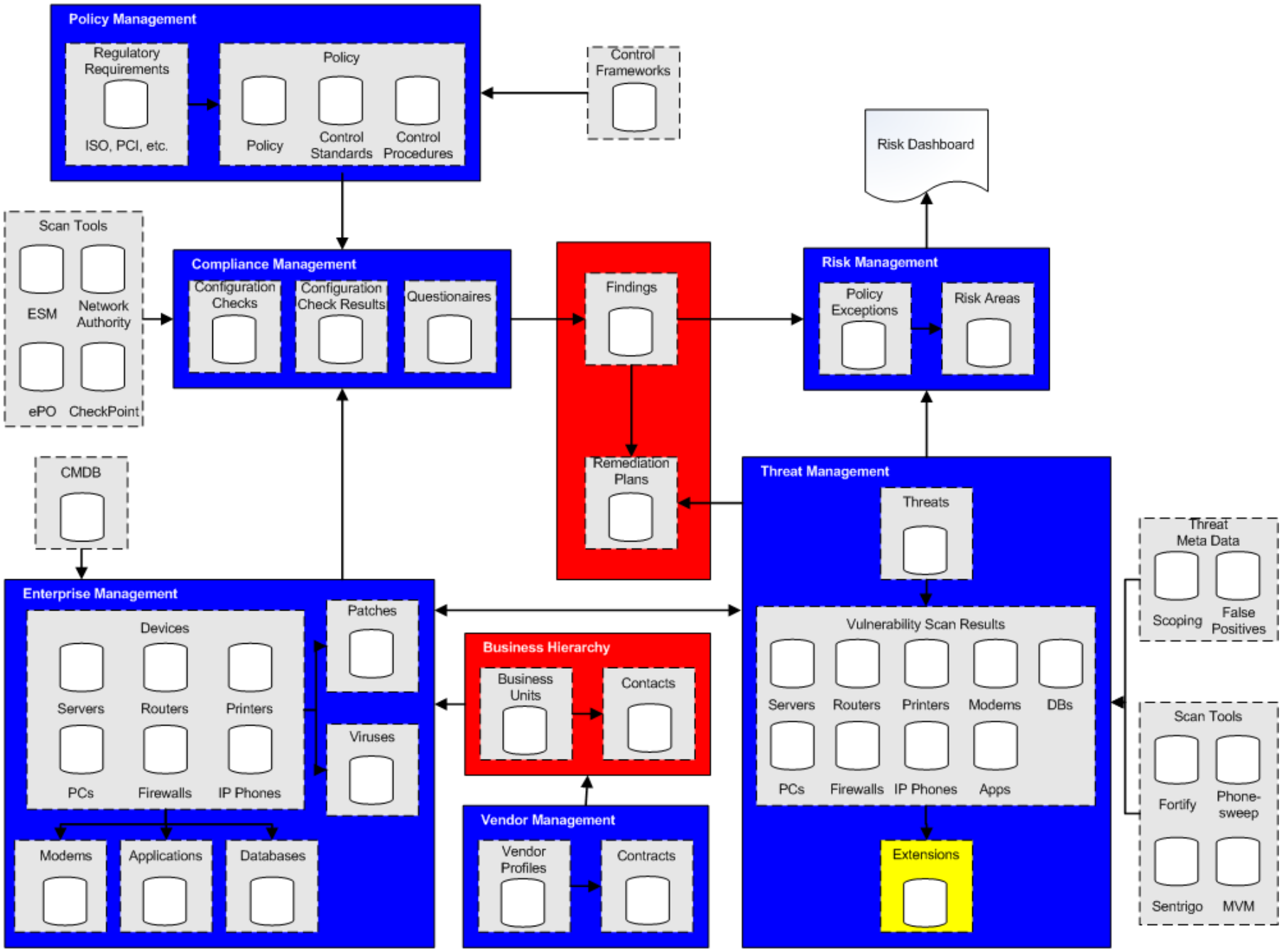
Security GRC at AT&T: Org Structure

- **Relationship Team**
  - Liaison for General Security Questions
- **Policy Team**
  - Maintain AT&T Security Policy and Requirements (ASPR)
- **Factory Team**
  - Conduct Security Assessments of AT&T Assets
- **Audit Team**
  - Liaison for Internal/External/Customer Audits
- **Vendor Management Team**
  - Conduct Vendor/Supplier Security Assessments
- **Risk Management Team**
  - Process Security Risk Management Agreements

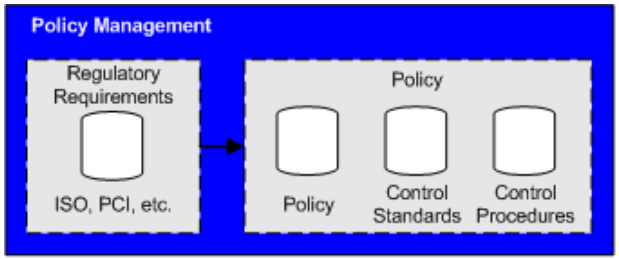
AT&T Multiyear Archer Roadmap

Rethink Possible

Archer at AT&T: Future State Vision

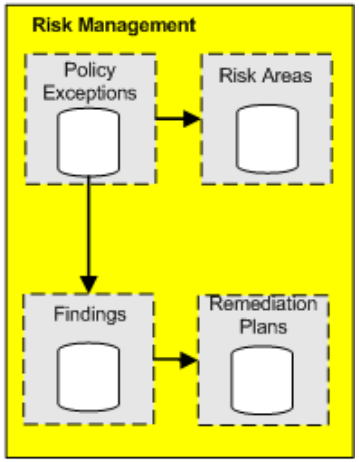


Archer at AT&T: Initial Deployment

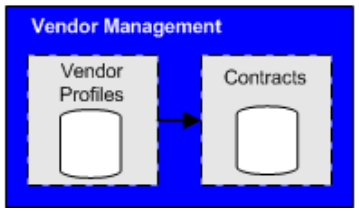


2

1



3

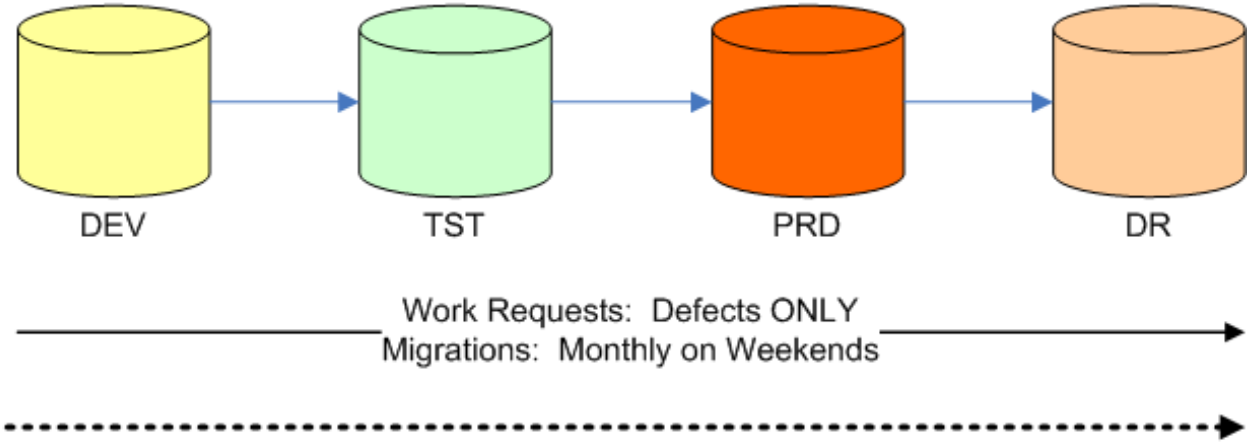


Archer at AT&T: Multi-Year Roadmap

Current State: AESOP Environments

Applications:

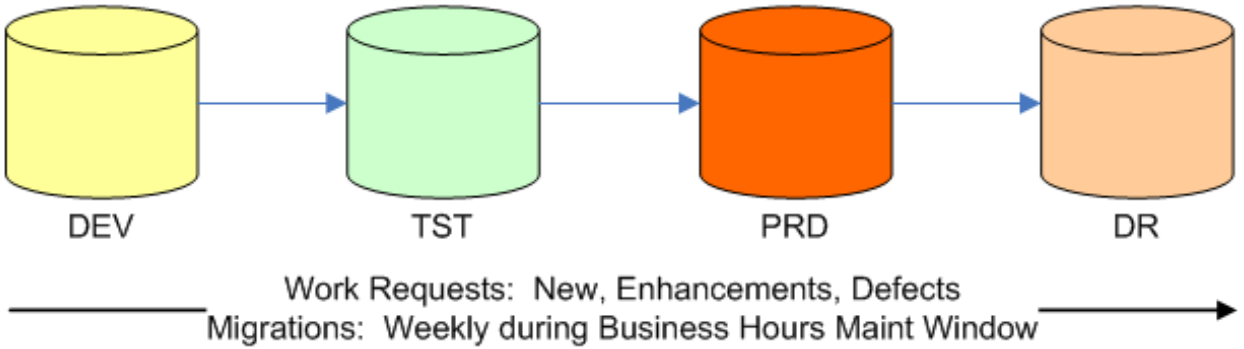
- ASPR – move to PM
- Ad Hoc - retire
- IPV6 - retire
- Metrics - retire
- TL-1 - retire
- Risk – move to RM
- SISR – move to VM
- Vendor – move to VM
- VLAD - retire



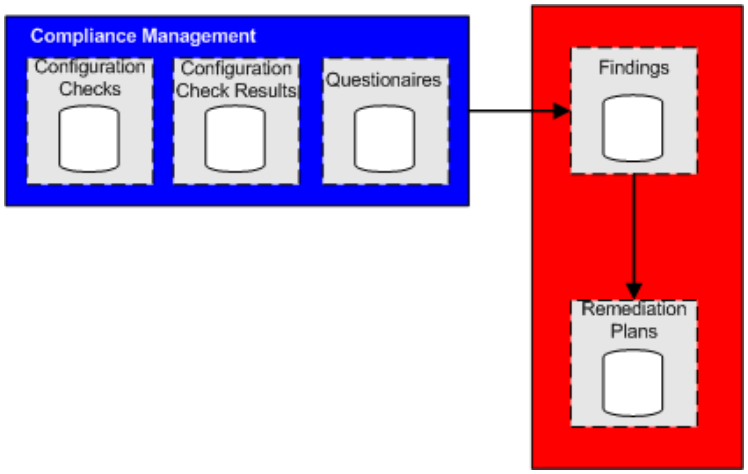
Future State: Compliance Environments

Solutions:

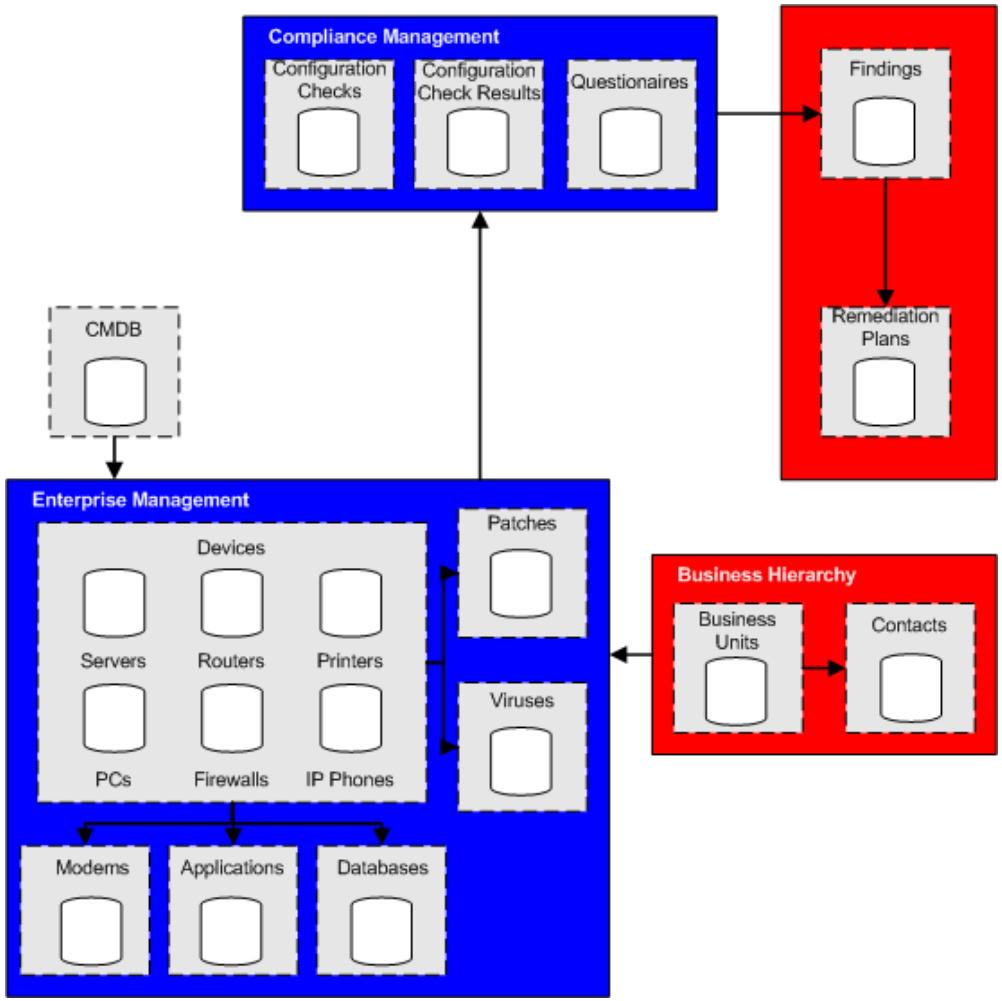
- PM - Policy Mgmt
- EM - Enterprise Mgmt
- CM - Compliance Mgmt
- TM - Threat Mgmt
- VM - Vendor Mgmt
- RM - Risk Mgmt



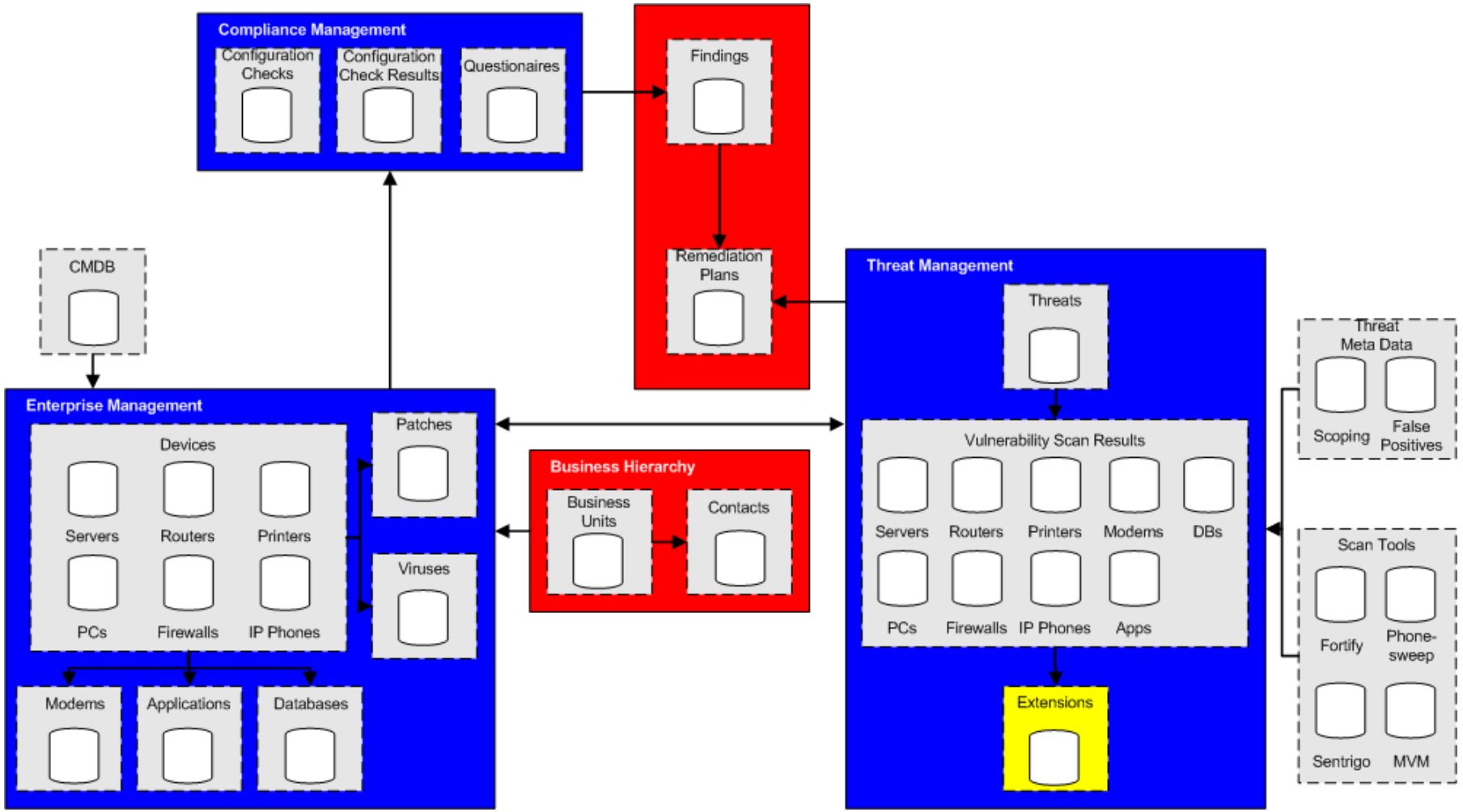
Archer at AT&T: Multi-Year Roadmap



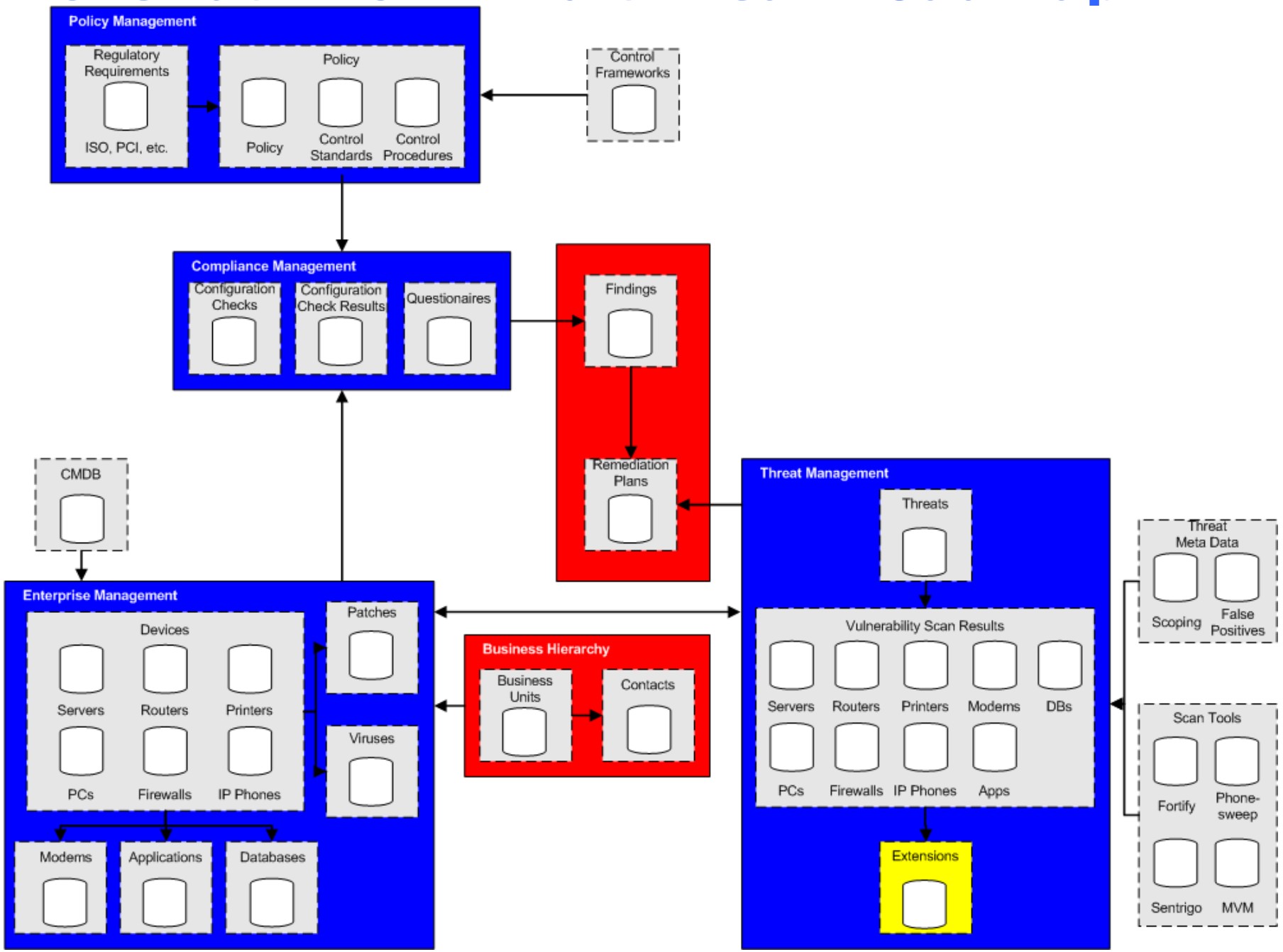
Archer at AT&T: Multi-Year Roadmap



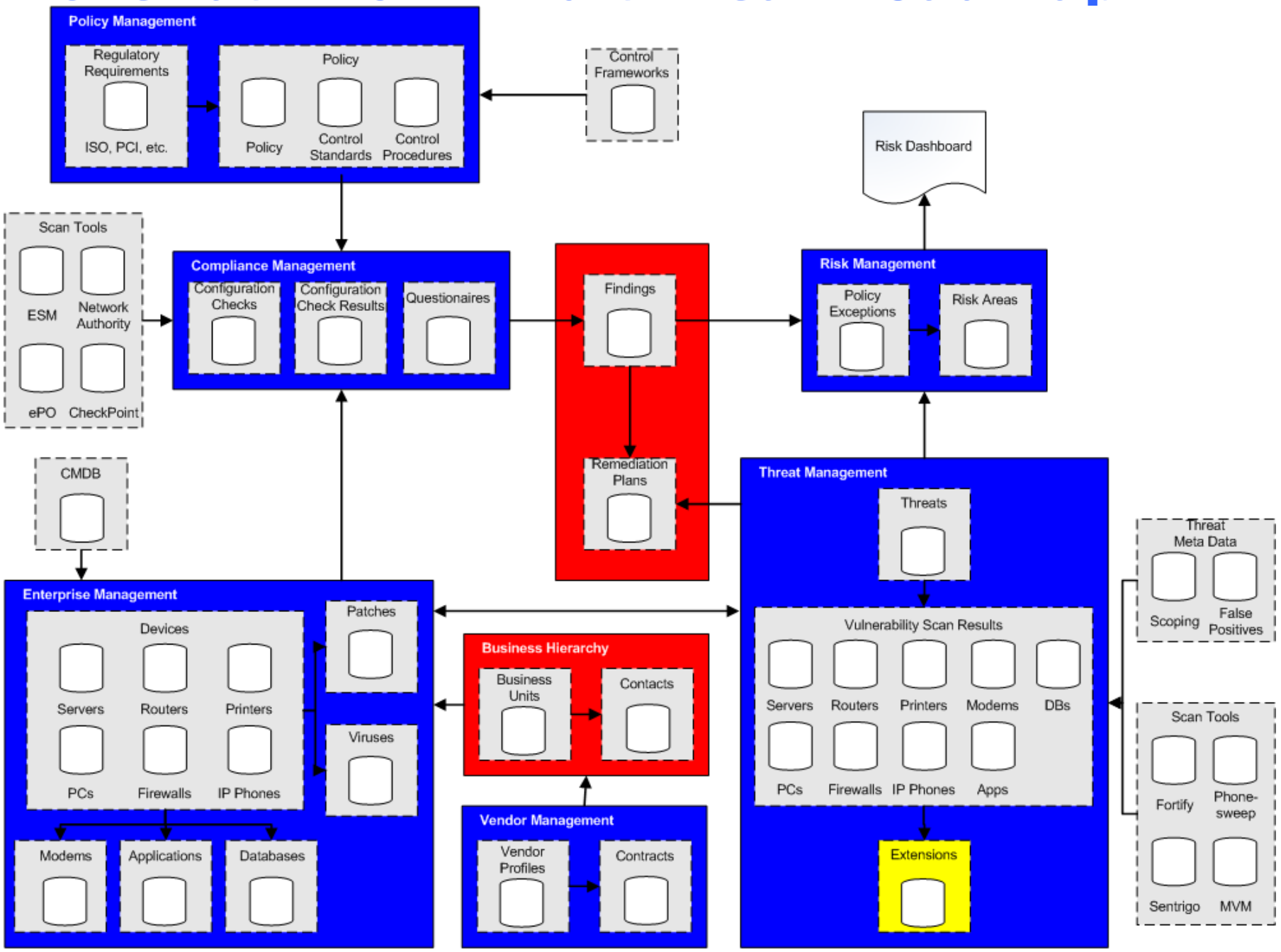
Archer at AT&T: Multi-Year Roadmap



Archer at AT&T: Multi-Year Roadmap



Archer at AT&T: Multi-Year Roadmap



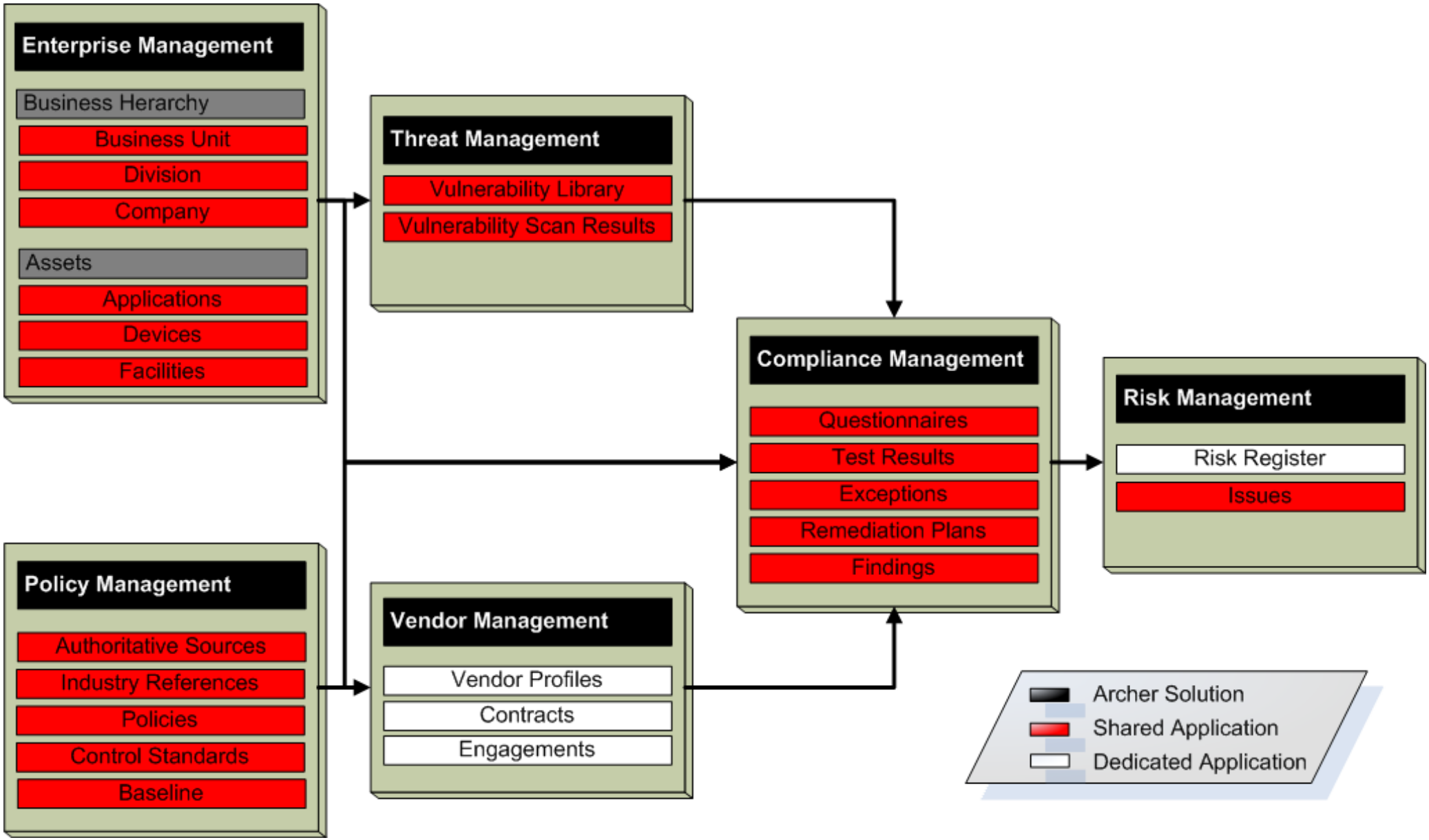
Lessons Learned

Rethink Possible

If We Could Do It Over Again…

- **Realize this is EXACTLY like an ERP implementation!**
  - Customizing the software will have a downside - long term maintenance.
  - The best way to take advantage of the built-in functionality is to use the software as 'vanilla' as possible. However, this can be a change management challenge.
  - When using several solutions, recognize the underlying applications are generally shared. Therefore, a change by one team will impact others.

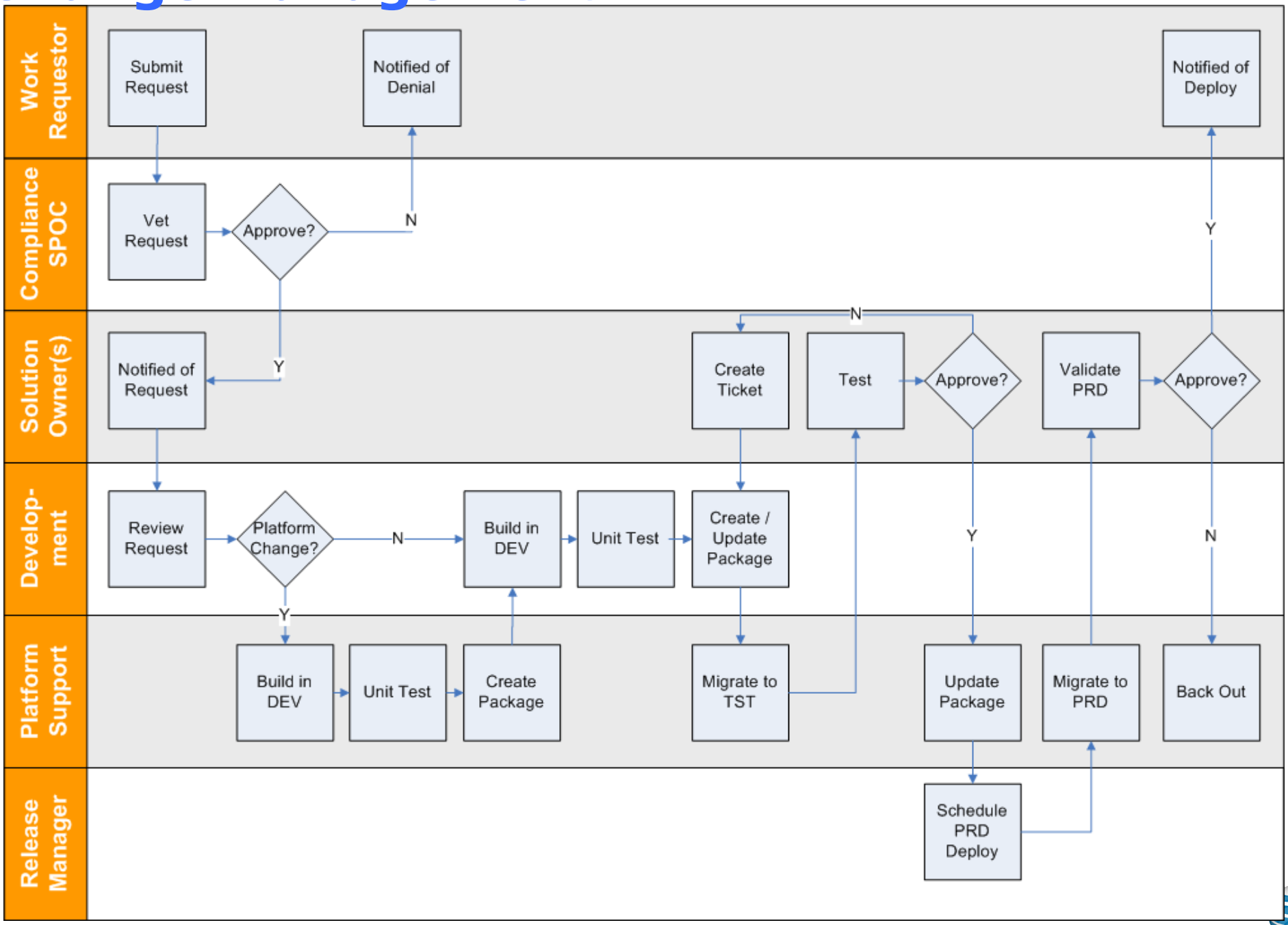
AT&T Application Ownership



If We Could Do It Over Again…

- **A simple, yet comprehensive change control process is key.**
  - If individual teams manage their own development, it will require significant effort to maintain solution integration.
  - To maintain integrity of the framework, certain functions may need to remain centralized.
  - An environment diagram is always a helpful tool.
    - NOTE: prior to v 5.0 objects can NOT be migrated and must be rebuilt in each environment!

Change Management



If We Could Do It Over Again…

- **Build a long term roadmap EARLY!**
  - This should not center around how many users or licenses are required.
  - This should focus on compliance processes Archer will be used to support and manual procedures targeted for retirement.
  - After developing a vision for the future process – evaluate which delivered Archer solutions fit best.
    - NOTE: A number of APPLICATIONS are shared across several SOLUTIONS, so there may be multiple ways to implement.
- **Designing SOLUTIONS in logical sequence will reduce customizations and speed deployment**
  - **AT&T Example:**
    - Foundation: Policy, Enterprise Management
    - Evaluation: Compliance, Threat, Vendor Management
    - Monitoring: Risk Management

QUESTIONS?

Rebecca Finnin
rebecca.finnin@att.com
678.451.3468

Rethink Possible