Security Architecture
- Week 3 -

Establishing the Security Architecture Business Context

Welcome

- Topics in the news
- Review of Week 2
- Week 3 Assignment
- Week 3 Lecture:
  - Establishing the Security Architecture Business Context
- Quiz

Business Context

What do we mean by

“Security Architecture

Business Context?”

Business Context

- Strategic Context
- Market context
- Competitive context
- Regulatory context
- Enterprise context
- Systems context
- Business Lifecycle context
- Budget context
- Product Lifecycle context
- Risk Profile
- Risk Tolerance
- Security Portfolio
- Security Projects
- SIEM organization

Strategic Context

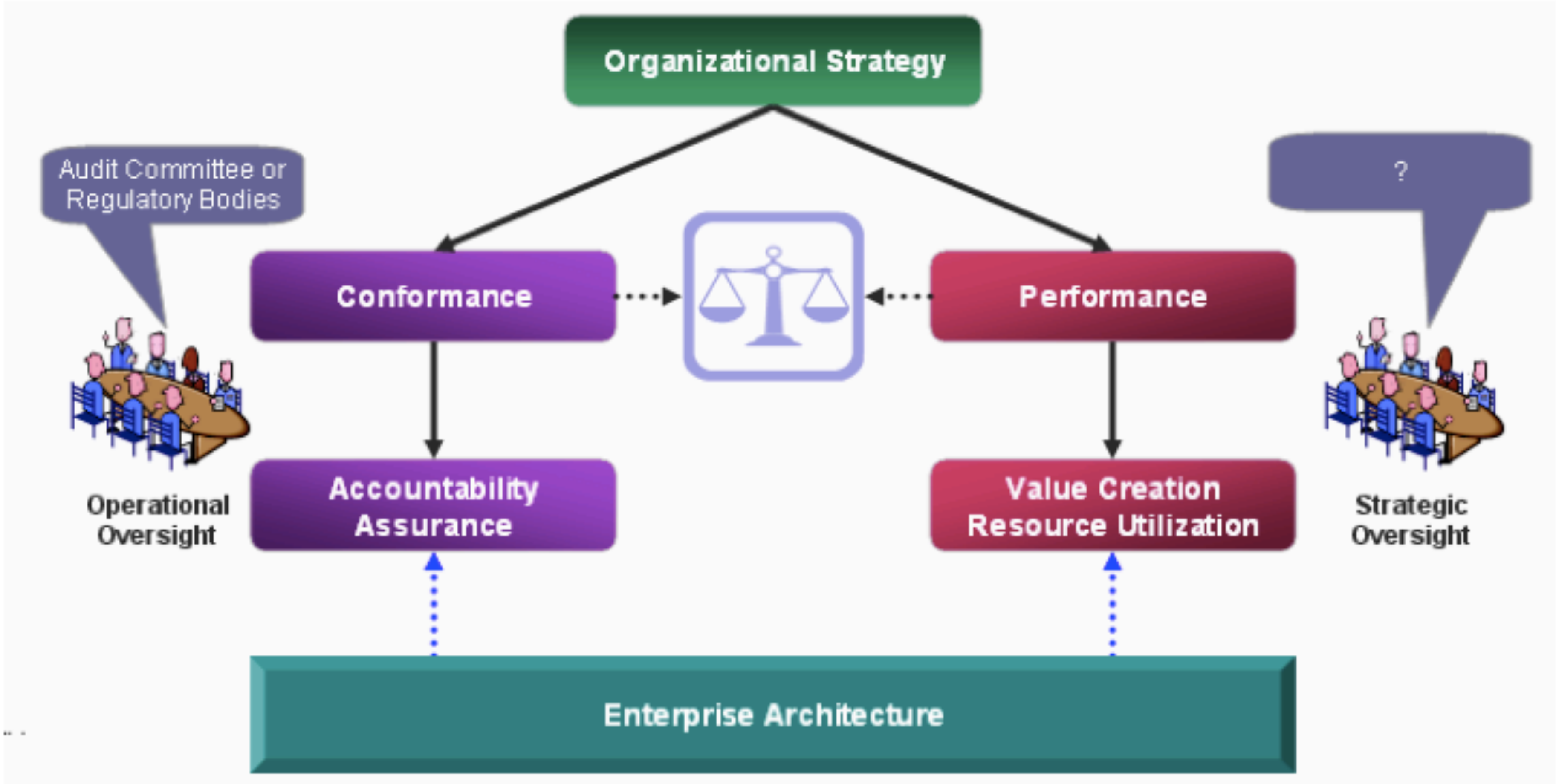

Figure 1. Organizational Strategy

Source: Sundararajan Vaidyanathan

Strategic Context

- Formal business strategy
  - finance
  - people
  - processes
- R eal life examples
  - Most business do not do this ☹
- Informal/historical
- Cultural - (steve jobs example)
  - engineering orientation
  - cost as a driver
- Individual agendas
- Outside influences
  - market
  - regulatory
- Management by objectives

Market Context

- Security can be driven by what your customers demand
- Market demands
  - Consumer electronics
  - Insurance
  - Healthcare
  - Retail
- Manufacturing - supply chain
- Changing customer concerns and requirements

Competitive Context

- What do my competitors do?
- Cost/benefit
- The security "arms race"
  - Banking
  - Retail
  - Credit cards
- Opportunism
  - Being prepared to take advantage of competitors issues
  - iPhone versus android security
  - Apple celebrity hack

Regulatory Context

- PCI-DSS
- HIPPA
- Sox
- State and local laws
  - wifi example
- Changing government requirements for disclosure
  - recent Obama administration cyber security initiative
  - State of the Union
- Ethic and business considerations

Enterprise Context

- Enterprise architecture
- Industry standards
- Defacto standards
- EP architecture
- Unique business circumstances
- Supply chain integration
  - EDI/b2b
- Payment systems
- Federal enterprise guidelines
- What you really find in business?
  - not planned … evolved
  - strategy under development
  - not fully documented
- Reference architectures
- Emerging Mobile frameworks

System Context

- Defacto standards
  - SAP
  - Oracle
- Microsoft standards
- Network environment
- Web capabilities
- Integration of social media platforms
- Sales systems
- Call centers
- Phone system integration
- Certificate authority
- PKI infrastructure

Business Lifecycle Context

- economic conditions
- mergers and acquisitions
- state fo company in maturity cycle
- state of products (subsudiaries in lifecycle
- BCG stages
- type of spendings
- timelines for impementations
- Priorities

Budget Context

- Timeframes are priorities are influenced by budget
- Yearly, quarterly budget cycle
- Staffing possibilities
- Systems implementation timing
- 0 based bugeting
- Typical incremental budgeting
- Changing market condition – re-priorization
- % as part of IT budget
- Budget trade-off
- Growth versus stability

Budget Context

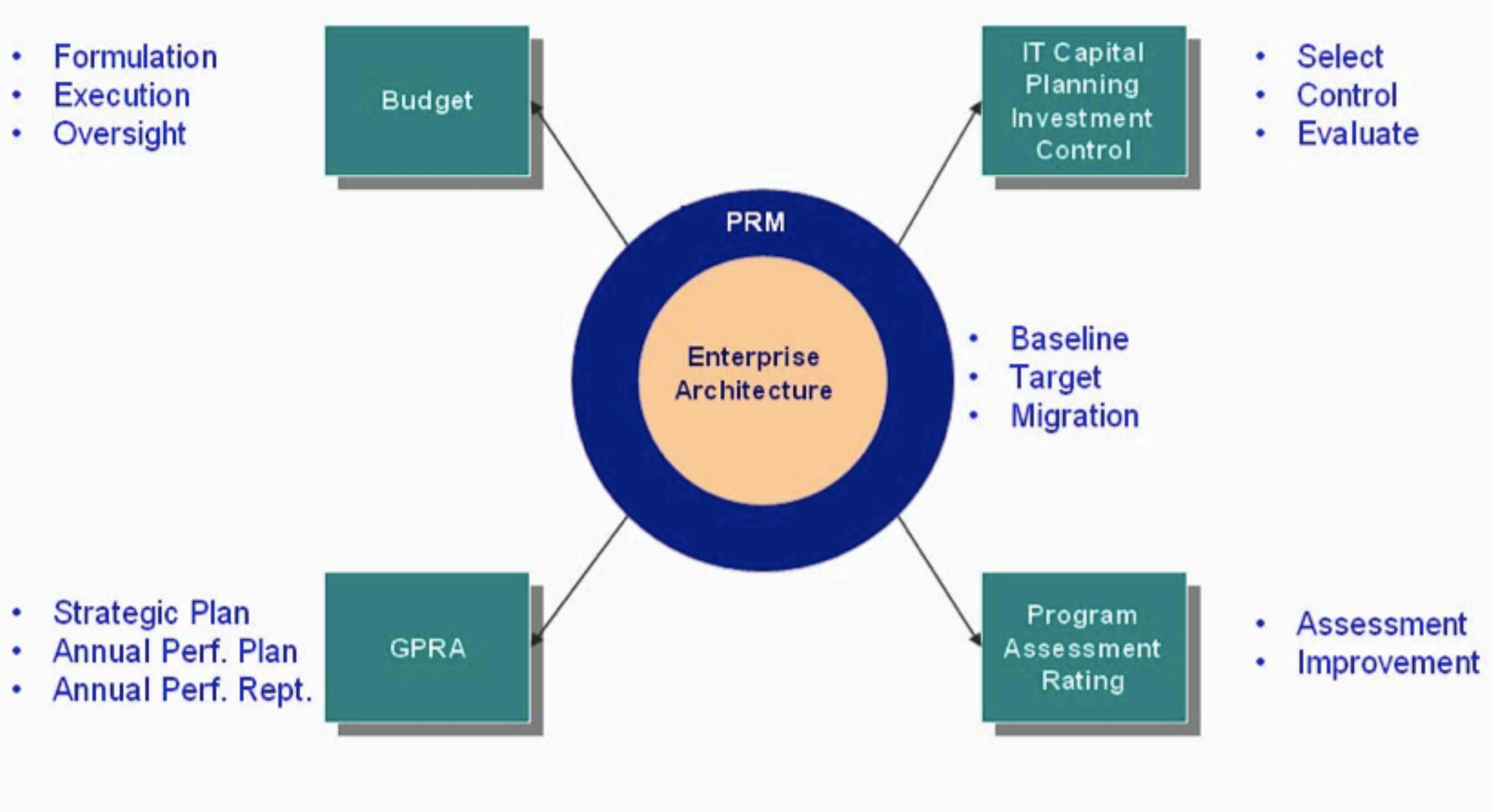

Figure 6. Strategic Management Processes

Source: Sundararajan Vaidyanathan

Risk Context

- Type of Enterprise
- Sensitivity of data
- Motivations of hackers
- Profitability Model
- Age of internal system and infrastructure
- Business lifecycle stage
- Media Profile/Visibility

Risk Tolerance

- Lifecycle stage
- Available resources
- Security awareness
- Sensitivity of data
- Perceived risk to operations
- Company culture

Security Portfolio

- Existing risk management operations
- Current priority of security objectives
- Maturity of organizations
- Executive engagement in prioritizing risk projects
- Sponsorship

Security Projects

- Existing initiatives
- Available resources
- Staffing model
- Company's project orientation
- Status of existing project in lifecycle
- Changing risk profiles
- Urgent response adaptations

SIEM Operations Approach

- Security information and event management
- Size of dedicated organization
- Level of experience and education
- Depth of event response planning
- Reliability of event management approaches (testing/ experience
- Agility of the organization in coping with urgent events
- Sophistication of data analytics
- Ability to gain management endorsement of rapid response
- Willingness to follow-through on event detection (target)

Quiz