

Energy Future Holdings



Luminant



Governance of Outsourced IT Services

Donna Hutcheson, CISA
Information Technology Audit Director
Energy Future Holdings Corp.

January 2009





Topics Covered in This Session

- Common failures in governing outsourced IT services
- Services with higher risk due to outsourcing
- Effectively governing outsourced IT services
- Integrating internal business processes, outsourced business processes and outsourced IT services with effective governance for all
- Guidelines for oversight of key performance indicators that truly measure the effectiveness of outsourced IT services



Background

- IT services typically outsourced
- Traditional activities involved in IT governance
- Roles and responsibilities in managing outsourced IT services

IT Services Typically Outsourced

Service	Pro	Risks
Logical Security	<p>Provider cost and maintenance fee distributed among clients</p> <p>Rapid updates with live monitoring</p> <p>Dedicated staff with up to date knowledge</p>	<ul style="list-style-type: none"> ➤ Loss or unauthorized access of data ➤ Data Integrity ➤ Failure to fully design, develop and implement enterprise security architecture ➤ Rely primarily on the firewall ➤ Failure to understand the relationship security has with the organization
Specialized service	<p>No in-house training</p>	<ul style="list-style-type: none"> ➤ Inability to support service during ongoing operation.
Desktop & server maintenance	<p>Remote control</p> <p>Consistent version control</p> <p>55% reduction in IT costs per employee</p>	<ul style="list-style-type: none"> ➤ Inaccurate/corrupted data and process integrity ➤ Inadequate built-in controls ➤ Few written procedures ➤ Inadequate unauthorized access protection ➤ Unapproved change implementation ➤ Failure to maintain the application ➤ Intellectual property theft ➤ Customer information - lost, manipulated or stolen ➤ Delayed service

IT Services Typically Outsourced (cont)

Service	Pro	Risks
Disaster recovery	<p>Frequently outsourced IT service</p> <p>Well established outsource service Service costs -low maintenance and does not require dedicated full-time staff</p> <p>Reduces risk of destroying company business.</p>	<ul style="list-style-type: none"> ➤ Hot/Cold recovery; ➤ Data access and integrity; ➤ Business/customer service disruption; ➤ Financial/external report misstatement; ➤ Lack of staff to support recovery; ➤ Access to recent back-up
Voice and data telecommunications	<p>Well established outsource service</p>	<ul style="list-style-type: none"> ➤ Illegal/malicious hacking; ➤ Denial of service attacks; ➤ Data corruption; ➤ Bottlenecks; ➤ Slow response times
Infrastructure operations	<p>No need for land or building to house equipment/personnel</p>	<ul style="list-style-type: none"> ➤ Inadequate risk assessment; ➤ Inadequate provider controls and ineffective monitoring ➤ Lack of strategic planning to meet buyer's needs ➤ Failure to maintain the system

IT Services Typically Outsourced (cont)

Service	Pro	Risks
Application Development and Maintenance	Do not pay provider during downtime No need to interview, hire, train team members No direct management of team members	<ul style="list-style-type: none">➤ Inefficiencies in the business process supported by the application➤ Inadequate contingency strategies for delayed projects;➤ Average outsourced projects are completed successfully and effectively 63% of the time

IT Services Typically Outsourced (cont)

Service	Pro	Risks
Help Desk – Internal/ Customer	Less knowledgeable technicians can resolve 80% of all help desk calls	<ul style="list-style-type: none">➤ Information may not be shared among service departments and providers➤ Conflicting behavior/solutions from the provider team➤ Difficulty in identifying performance trends➤ Inability to respond quickly to changing market conditions➤ Loss of revenue from customer dissatisfaction➤ Customer requirements may be misunderstood➤ Provider staff may not be trained to meet customer needs effectively➤ Inaccurate reporting➤ Provider employees may breach organization standards related to security and confidentiality➤ Incomplete/inaccurate recording and communication of problem – common or critical➤ Cultural differences may interfere with escalation of problems to appropriate staff➤ Key decision-makers may not be aligned with day-to-day operations



Traditional Activities in IT Governance

- Contract Management
- Service Level Metrics and Reporting
- Business Project Liaison with Service Provider
- Annual Review of SAS 70s and Other Industry-specific Regulatory Compliance
- Routine Meetings to Resolve Issues
- *Participation in Change Management Mtgs*
- *Audit Escrow Accounts*

Roles and Responsibilities

Buyer

- CIO – Chief Information Officer
 - coordinate internal technology strategic direction
 - coordinate information technology as infrastructure for all business units
 - manage external partnerships
 - improve services to employees and partners
- CTO – Chief Technology Officer (Business Specific)
 - provide a technical voice in strategic planning
 - reduce operating costs
 - manage application specific solutions
 - liaison with business owner
- CSO – Chief Security Officer
 - provide IT security vision, strategy and programs
 - manage cyber security, standards, data and network asset protection

Information Technology Leadership is bigger than a single service provider relationship

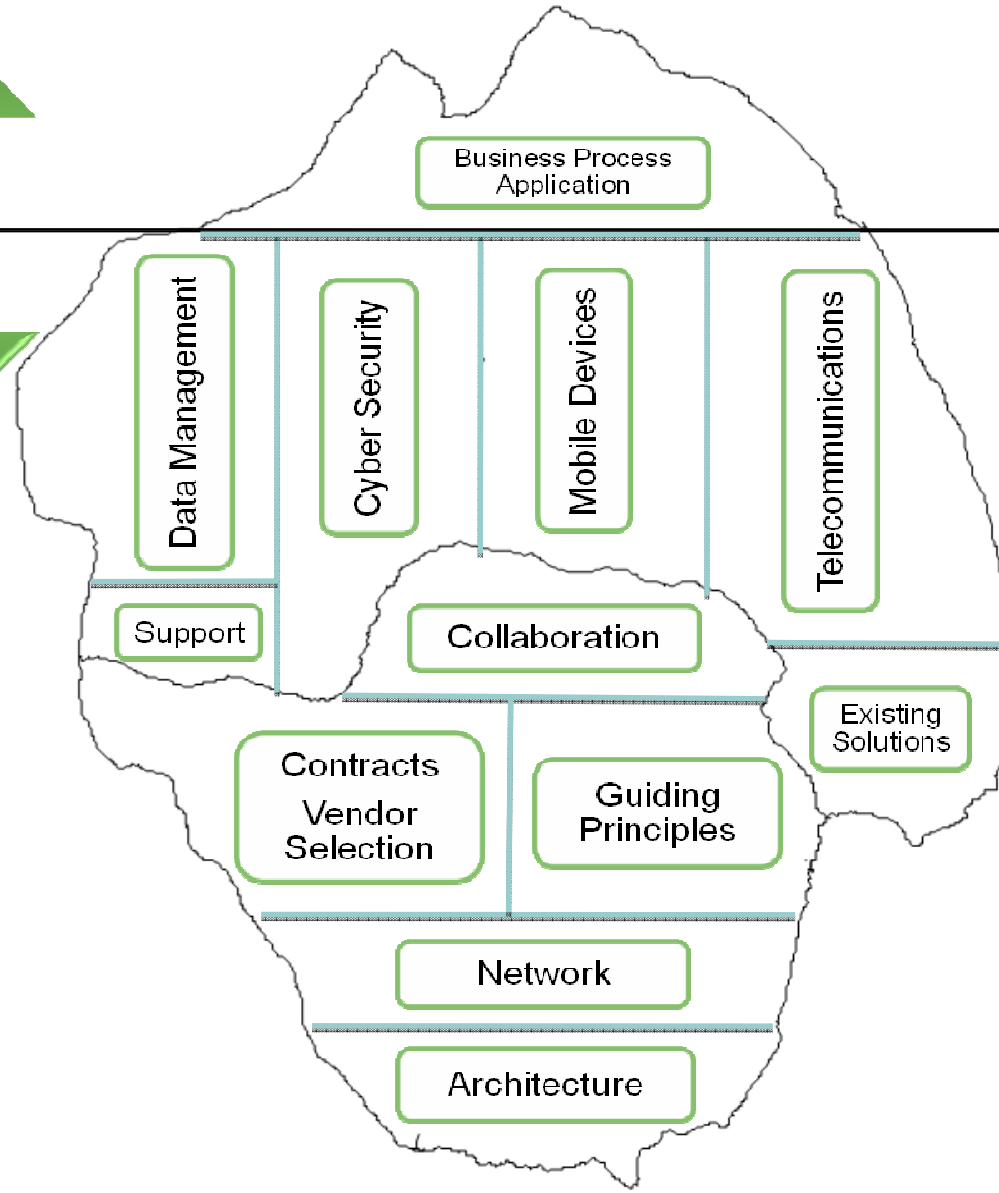
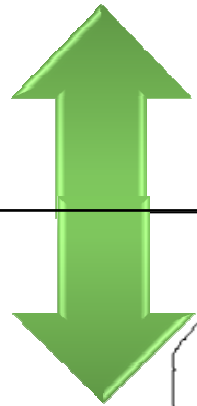
Service Provider

- Service Delivery Managers
 - relationship management
 - ensure service levels
 - communication with buyer management
 - coordinate services across silos
- Service Operation
- Administrative Manager
 - measurement of metrics
 - reporting
 - billing
- Project Management Office
 - prepare proposals
 - provide oversight of project activities
 - change management
 - communicate with business owner
- *Security Representative to communicate with Buyer CSO*

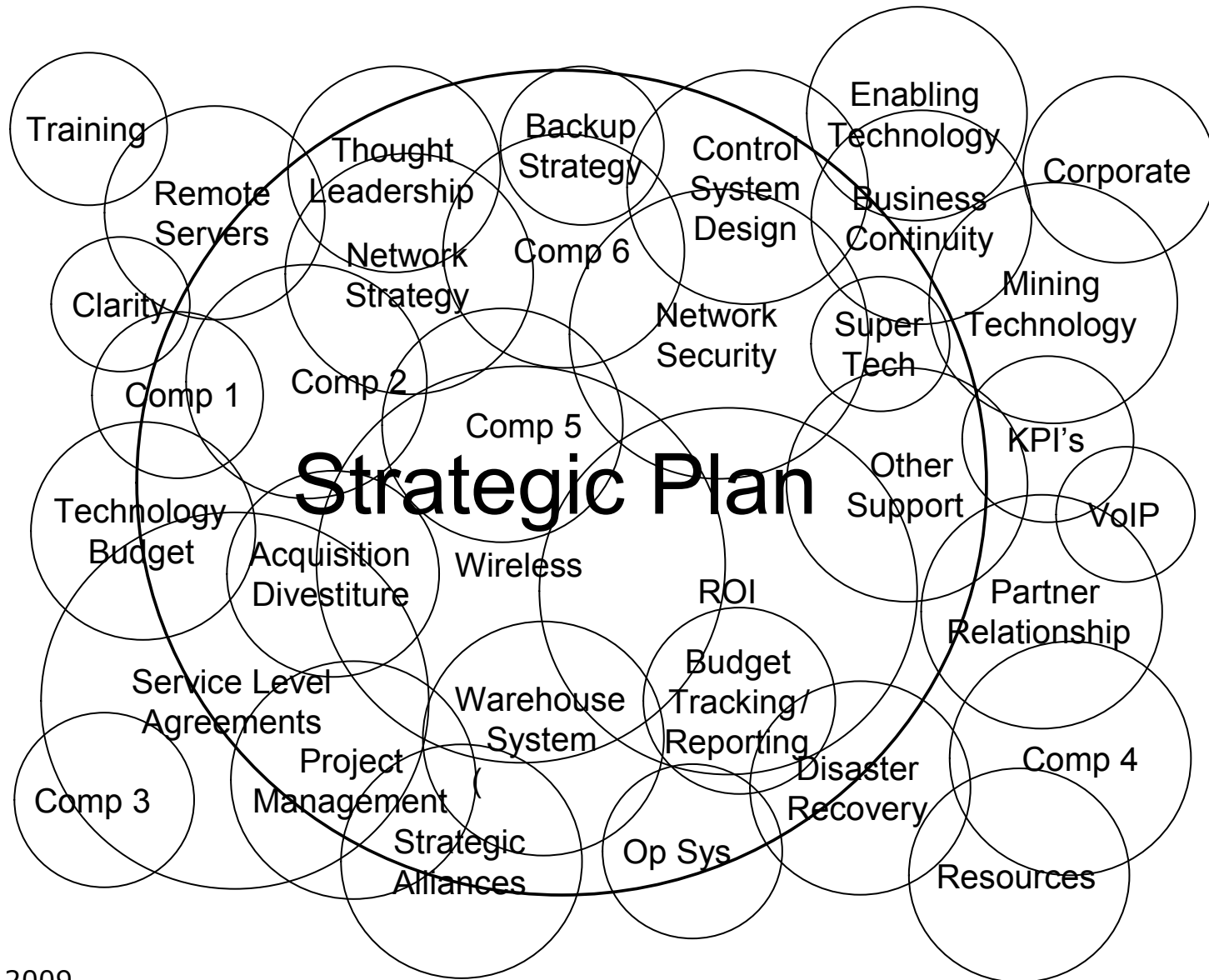
IT Governance (more than meets the eye)

What

How



An IT Strategy is Critical





Business Expectation Management

- BPO = Business transactions/processes
- ITO = IT Services
- Positive changes in ITO = positive changes in the business processes
- Negative changes in ITO = negative changes in the business processes
- Broken or ineffective IT processes that are outsourced will not be miraculously repaired
- Buyer is always responsible for what, where, who, and how
- Only “you” know your business
- Only “you” are accountable for compliance with laws and regulations



Common Failures in Governing Outsourced IT Services

- Negotiating too hard to a least cost scenario
- Misplaced haste to get a contract in place
- Lack of an exit strategy
- Failure to control legal compliance
- Failure to plan for a long-term strong relationship
- Negotiating and managing from an “Ivory Tower”
- Ignoring performance details



Common Failures in Governing Outsourced IT Services (cont.)

- Impairing your ability to "Get Up and Walk Away"
- Burning bridges with other partners
- Failure to monitor service (business)
- Relinquishing control/oversight (business)
- Failure to review Outsource Service Providers' internal controls
- Failure to audit services provided
- *Failure to routinely review providers' financial statements*
- *Validating the destruction of confidential data when changing providers*



Governance Risks

- Strategic direction
 - Who determines the problem to be solved?
 - Motivation to find best functional strategy vs. cost effective strategy?
- Total costs
 - Baseline
 - Maintenance
 - New projects
 - Decommissioning services/applications
 - Adding new services/controls



Governance Risks (cont.)

- Legal and regulatory consequences
 - Financial controls (Sarbanes Oxley for U.S.)
 - Data privacy (global issue)
 - Effective controls assertion (SAS 70)
 - Industry specific governing committees and standards

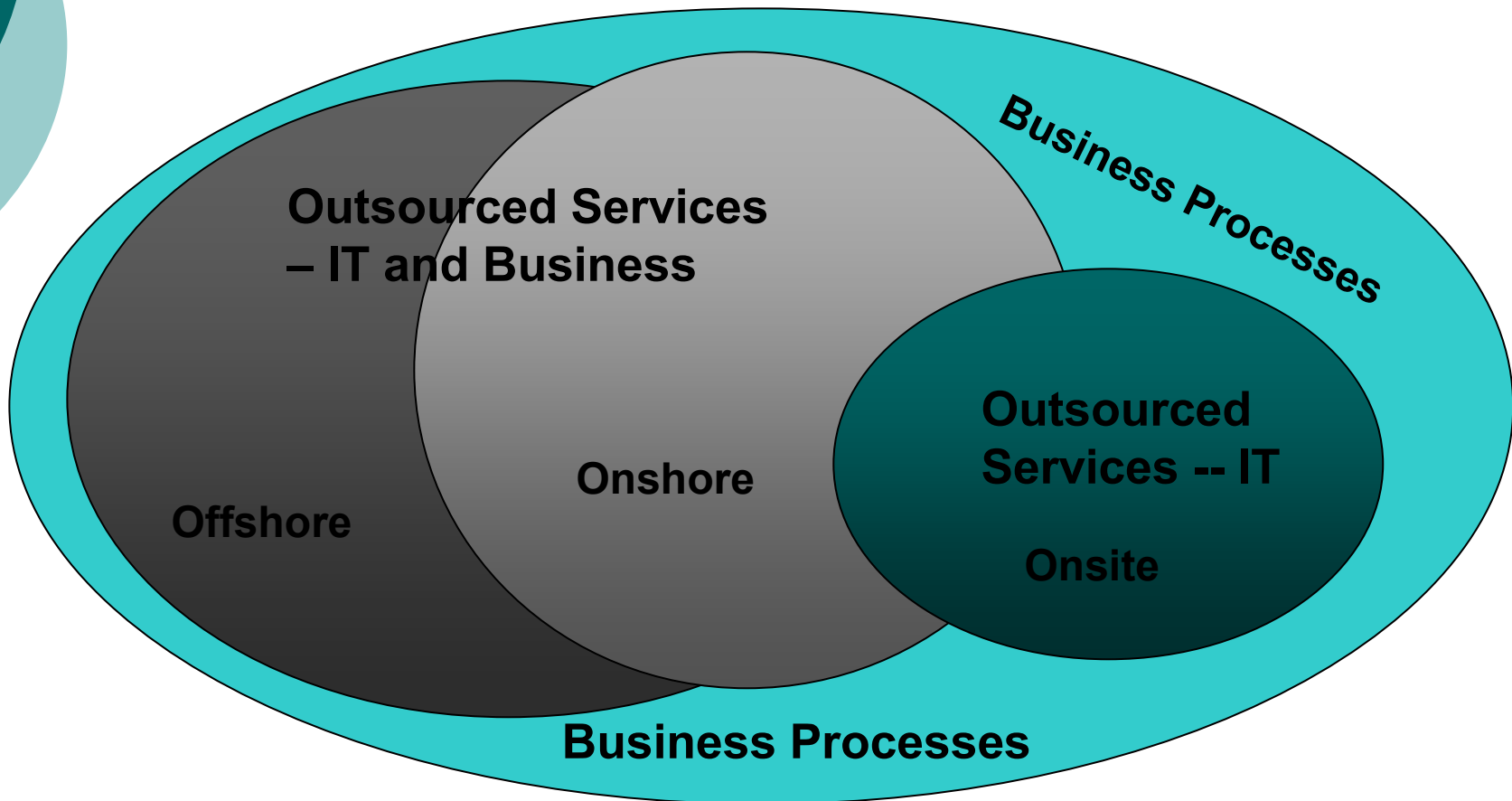


Effective Governance Outsourced IT Services

Active strategic guidance of the process is imperative to achieve monetary and functional value for corporate stakeholders. Each governance strategy should address:

- *What problem are we trying to solve?*
- *What is the cost?*
- *What is the value to the company?*
- *Do the services provided negatively impact required business functions?*

Integrating Internal Business Processes, Outsourced Business Processes and Outsourced IT Services





Key Performance Indicators and Metrics for the Effectiveness of Outsourced IT Services

➤ Today

Examples:

- *% time servers available*
- *% time network available*
- *# of IT help desk calls*
- *Average time to answer*
- *Customer satisfaction*
- *# mhz volume*
- *# applications*
- *# space Terabytes*
- *# email messages*

➤ Future - *What should we be looking for in metrics?*

Examples:

- *% quarantined spam?*
- *Firewall connection blocks?*
- *Total patches vs # deployed?*
- *# viruses blocked at gateway vs # viruses successfully detected?*
- *# of "heartbeat accounts" vs # service/shared accounts?*
- *# of incidents?*
- *# of B2B VPN connections*
- *# of application projects and status?*
- *# of infrastructure initiatives and status?*

Research results from eight industries

Source of Service	<u>Primary IT Control Issues</u>
All IT Services within the company	Undocumented policies and procedures Segregation of Duties conflicts (inconsistent among business units)
Mixed vendor outsourced services	Inconsistent policies/procedures Inadequate SAS 70 testing Network Security vulnerabilities
All IT Services outsourced	Inadequate IT governance and strategies Provider outsourcing to other vendor, but not passing along policies Inadequate SAS 70 testing Intellectual property theft Inadequate communication and metrics Network Security vulnerabilities

Research results from eight industries

Industry	<u>Primary IT Control Issues</u>
Retail	Segregation of duties and documented procedures Network security
Manufacturing	Application interface controls
Service	Inconsistent processes across business units Network security
Energy	Network security Access controls
Health	Regulatory compliance Network security
Real Estate (REIT)	Policies, documented procedures
Petroleum	Network security Inconsistent processes across business units/locations
Financial	Regulatory compliance Network security

Risks of Not Conducting Routine IT Audits

(regardless of sourcing)

- May not understand single points-of-failure in an otherwise secure environment
- May not understand what impact these failures may have on the infrastructure (e.g. can provide a path or direct access to sensitive business data)
- Could impact business goals and objectives (e.g. meet regulatory compliance)

Slide 22

DH1

Too apple pie. Give examples of what they might miss as a single point of failure, give diagram of how attacks may happen.

Donna Hutcheson, 5/5/2008



For More Information:



Donna Hutcheson, CISA

ISACA North Texas University Relations Director
ISACA International Academic Relations Committee
Director, Internal IT Auditing

Donna.Hutcheson@energyfutureholdings.com

Energy Future Holdings



Thank you!

January 2009

