FEDERAL ENERGY REGULATORY COMMISSION STAFF REPORT ON

INFORMATION TECHNOLOGY GUIDELINES FOR

POWER SYSTEM ORGANIZATIONS

PREPARED BY GESTALT, LLC

Gestalt

APRIL 2005

Executive Summary

Introduction

As the electric industry faces reorganization and modernization, one of the traditional reliability and cost-saving challenges it faces involves the telecommunication interconnectedness among utilities within power grids and among grids in large sections of the nation.

A special concern for the Federal Energy Regulatory Commission (FERC) is that as the electric industry plows ahead into the Digital Age, it is increasingly reliant on automated information technology (IT) operations because human operators simply cannot act quickly enough to react to cascading failures in power grids. This was a key problem that contributed to the August 2003 blackout that left 50 million people without power in the northeastern quadrant of the United States and in adjacent Canada.

Unfortunately, one characteristic of sophisticated IT programs is that they are prone to failure. In addition, when companies forego off-the-shelf applications and instead use customized IT platforms, the resulting one-off program can be costly to develop and operate, and problematic in interfacing with other programs.

Last year, FERC hired consultant Gestalt LLC to study these problems. In its report, Gestalt cited 2004 survey results from the Standish Group, a Massachusetts-based research group established in 1985 that annually surveys IT projects and their performance. Since 1994, Standish Group has compiled research on 40,000 IT projects.

In its 2004 survey, the Standish Group found that only 34% of IT solutions succeeded. The rest failed completely (15%) or substantially (51%), meaning they failed to meet schedule, budget or functionality commitments.

The reasons include having poorly qualified managers trying to force ahead IT projects without proper preparation.

"Although fast-tracking can be done, it is a recipe for disaster when the business, functional and technical requirements are not clear," said Gestalt. It added that "six of the 10 historical reasons for project failure are associated with poor project management skills and unrealistic expectations, objectives and time frames."

Not surprisingly, the Gestalt report noted that the electric industry is no more immune to IT project failures than any other industry.

This obviously is a concern to the FERC, which, while it looks at many electric industry issues, nevertheless views as chief among them the reliability of electric grids, especially after the August 2003 blackout. In addition, FERC is concerned about the economic efficiency of the power industry, especially as more emphasis is placed on regional interconnections. FERC has vigorously promoted the development of regional transmission organizations (RTOs) and independent system operators (ISOs), but its reliability and economic concerns apply equally to all electric grids throughout the nation.

In its review of IT use in the power industry, Gestalt reported that market implementations have been delayed and more expensive than estimated. IT staffs and operating budgets have ballooned. New tools for system operators have been slow to evolve and software vendors have not delivered significant innovation in recent years.

To realize the benefits of competitive markets and open access as quickly as possible, industry stakeholders put tremendous pressure on technology development and implementation programs. As a result, said Gestalt, these projects went forward without the appropriate levels of business alignment, justification, project management rigor and adherence to proven technology development methodologies.

Management, regulators, board members, stakeholders and technology vendors should learn from the experience of missed deadlines, exceeded budgets and unmet expectations.

Fortunately, the situation is better today than it was in past years.

In its 2004 survey, while the Standish Group found that 15% of IT projects failed completely, that was an improvement over its 1994 results showing that 31% failed completely.

There are clear signs that project managers are learning from experience. Standish Chairman Jim Johnson attributes the improvement to several factors. "The projects have gotten a lot smaller," he said, adding, "Doing projects with iterative processing as opposed to the waterfall method is a major step forward and people have become much more savvy in project management. When we first started the research, project management was a sort of black art. People have spent time trying to get it right." [1]

Happily, the power industry has been part of this improving trend. For example, PJM's integration of Commonwealth Edison and American Electric Power went well from an IT perspective. And, ISO New England successfully implemented its standard market design (SMD).

Working in concert, power system operators, regulators, boards and vendors can create an environment in which significant and continuous improvement is part of the fabric of these organizations.

Industry software developers and other stakeholders can stay within budget, meet deadlines and fulfill expectations if they take to heart four key combinations of policies, processes and procedures to:

(1) set clear expectations and establish realistic schedules;

(2) develop common architectures, standardize technologies and avoid expensive customization;

(3) establish standardized IT governance, project management, technology development and vendor management; and

(4) require information technology management best practices.

The following sections describe how to do this.

Set Clear Rules and Schedules

[1] www.Softwaremag.com/ Software Magazine - Standish Project Success Rates Improved Over 10 Years, Jan. 15, 2004.

For nearly a decade, delays have seemed inevitable for projects that involve new regulations, market designs, market rules and technology standards. Vague, unclear or unfinished business rules inevitably lead to stalled projects and delayed implementations. Software may not be configured to support specific functions until the basic market design decisions are made. The result of design changes or stalled decision-making causes overruns and implementation delays. Project teams on large projects can easily reach 100 or more members; delays can cost as much as $1 million or more per month.

To implement complex software designed to support reliability or market operations, IT organizations must undertake a significant amount of detailed business process and rules development work. As a rule of thumb, expect that a large complex project, like the implementation of a new electric market, will take twice as long to implement if decision-makers try to fast track the project and under-allocate the time and resources needed for the planning effort, fail to employ a phased implementation approach and do not lock down the business rules early in the project. The schedules for many IT projects associated with the creation of new organizations and the implementation of new regulations are established by regulators, managers and politicians without first taking stock of the effort required to specify, integrate and implement the technology. Unrealistic deadlines and aggressive schedules are set and the project team is asked to do what ever it takes to get it done.

As noted above, while fast tracking can be done, it also can be a recipe for disaster.

Board members, management and regulators can all take part in ensuring that the development of clear expectations and realistic schedules by:

- implementing common reliability standards and market designs whenever possible;
- prioritizing business objectives and removing conflicts among them;
- enlisting experts early in the project to estimate the time and cost to implement significant changes, identify critical path items and prioritize objectives;
- preventing projects from starting without a realistic schedule and well-documented project plan that identifies contingencies and risks;
- setting interim milestones and decision lock-down dates, and encouraging phased implementations so that incremental progress can be made even when full

agreement on future design aspects and business objectives has not been reached; and

- monitoring progress against a plan, encouraging honest debate and discussion of risks and agreeing to adjust expectations accordingly.

Use Common Architectures and Avoid Customization

Power System Operations (PSO) organizations can reduce initial and on-going support costs, enable reuse and ensure interoperability by designing applications that incorporate common and open architectures, protocols and platforms, and that take advantage of standard technologies to avoid customization.

Applications development and integration costs can be significantly reduced through the use of open architectures and technology standards. Industry stakeholders realize this and have begun working together to develop reference architectures, standard data definitions and common data transfer protocols. These groups must continue to work together to:

- adopt open architectures that are hardware and database independent to promote data exchange and increase interoperability;
- adopt industry wide information technology standards to reduce costs and increase interoperability, and extend the life span of applications; and
- develop more flexible solutions that are based on modular designs and use nonproprietary languages and off-the-shelf software when appropriate, and are positioned to leverage Web services in the future.

Additionally, application implementation project costs increase disproportionately as the amount of customization increases. Thus, if the amount of customization increases by 10%, the cost of the project will increase by far more than 10%. New-application implementation costs and implementation durations can be minimized by adopting common business processes, using standard configurations, and limiting the amount of customization.

Look for ways to recycle and reuse software and applications. While the ability of one PSO to reuse the applications developed for another PSO is limited by commercial and practical operations factors, the movement within the industry to create common architectures and data definitions will make reuse a more viable option in the future. Use of modular design will help cut development time and costs.

Use Standardized Management and Development Rules

PSO organizations require complex technical environments and large technical organizations to perform the engineering analyses and process the transactions necessary to manage reliability and administer markets. IT organizations must be focused on achieving operational excellence and must adopt a mindset of continuous improvement.

However, because of the cost-sensitive environment in which the PSOs operate, IT organizations need to be fiscally prudent in their pursuit of operational excellence.

The implementation of technical best practices, therefore, needs to be carried out within the context of cost minimization. As the responsibility of PSO organizations is expanded, additional expenditures may be warranted as the criticality of operations increases.

However, many best practices do not require large expenditures of funds but rather are dependent on, and a function of, a disciplined, process-centered organization.

Information technology governance, adherence to a defined system development life cycle (SDLC) methodology, comprehensive project management processes and strong vendor management are all best practices necessary to provide the discipline required to implement technology projects on time and within budget. A recent study by MIT[2] of more than 200 public companies found that companies with established IT governance practices show on average 20% greater earnings than companies that do not have an established IT governance structure.

Additionally, the Standish Group studies indicate that development initiatives fail when project management and development methodology best practices are not followed.

[2] ComputerWorld, Sidebar: MIT Researchers Tie Good Governance to Higher Profits, July 12, 2004, http://www.computerworld.com/managementtopics/management/story/0.10801.94458.00.html.

Studies have shown that the benefits of adhering to established governance policies, project management processes and technology standards and methodologies are realized by companies in all industries, from telecommunications to banking and defense, and apply to the power system industry as well.

Interconnected transmission grids and electric power markets are complex, highly dependent upon real-time data, serve multiple stakeholders and have unique characteristics.

These are, however, characteristics that are common to nuclear power plants, global telecommunications networks, distributed command centers, space exploration programs and a host of other critical systems and processes. PSO organizations are not so unique that they should not adhere to best practice expectations.

Generally within the PSO industry, there are very few functions that do not have commercially available solutions. Business intelligence functions that involve data warehousing and analytics and market settlement systems are a noted exception.

Establish a Best Practices Culture

Board members, managers and regulators can encourage the adoption of best practices by asking the right questions when project or budget approval is requested, rate relief is sought, tariff approval is required or significant regulatory change is desired.

A few of the more important questions include:

Is this project necessary?

In general, IT applications and infrastructure should not be replaced unless the business needs they were intended to support can no longer be met cost effectively. This would include the inability to meet the functional requirements of the business, the cost to maintain the technology is significantly higher than alternatives or the technology is obsolete and can no longer be supported.

What metrics show that this project is needed or the expense is required?

To perform at a high level, IT organizations need to institutionalize the process of measuring the performance of their organization, technology and vendors. Performance metrics should be captured in four critical areas:

(1) system and application performance,

(2) IT service delivery,

(3) project delivery, and

(4) cost.

How was the Buy vs. Build decision approached?

No decision regarding the choice of buying a commercial off-the-shelf solution or building a custom-made application should be made until the business needs are well articulated and documented, user requirements are determined and planning and analysis are completed. Any decision to build new reliability or market applications completely from scratch, rather than to reconfigure or customize existing vendor products, should be scrutinized and validated. In many cases the convergence of market designs has created the ability to reconfigure and customize vendor offerings at a lower cost than a complete new build.

Have you considered using someone else's solution?

While the ability of one PSO to reuse the applications developed for another PSO is limited by commercial and practical operations factors, the movement within the industry to create common architectures and data definitions will make reuse a more viable option in the future. An effort to use an existing solution or borrow significant portions of another PSO's solution should be made. One example of this was the ISO NE implementation of SMD, which was modeled after PJM's design.

Should this project be abandoned?

Given the large financial outlay associated with application development projects, there is a tendency to look back at the sunk costs and conclude that an investment of this magnitude cannot be abandoned, regardless of the cost to complete. This is erroneous decision-making, and often obscures the true viability of a project. Every project plan should incorporate cost, scope and schedule controls and have an exit strategy to avoid runaway spending.

How will you manage the vendor?

The limited number of vendors in the reliability management product sector may not be an issue because the size of the market limits the number of vendors that could remain viable.

However, the potential over-reliance on one or all of these vendors by a PSO may introduce risk. To mitigate the real or potential risks of dependency on one or more reliability/security management application vendor, PSO organizations should:

- develop an applications portfolio that contains a range of reliability management products that fall along the buy vs. build continuum;
- move towards an industry standard common architecture;
- create and maintain current business and technical requirements and design documentation of their reliability management functions;
- invest in in-house technical experience with critical applications to be able to triage operations problems and facilitate and manage application modifications, interfaces and upgrades;
- create appropriate organizational structure; and
- develop long-term strategic partnerships with their critical reliability management application vendors that are based upon trust, shared risk/reward and mutually understood goals and objectives.

Conclusion

The information, recommendations and best practices described in the accompanying report should be used by regulators, board members and power system operators as a starting point on the path to better technology implementation budget, schedule and functional performance.

There are no silver bullets and not all of the recommendations apply to every situation, but, with a common vision, a concerted effort from all stakeholders and the proper oversight, the industry will gain reliability while avoiding project delays and cost overruns.

1. Table of Contents

Table of Figures

II. Introduction

This report is submitted to the Federal Energy Regulator Commission (FERC) by Gestalt as the final deliverable in a project initiated by FERC to develop Information Technology (IT) management best practices for Power System Operations (PSO) organizations and to address critical PSO industry IT issues. This Introduction provides an overview of the project objective, approach, report structure, and recommendations; while the body of the report provides an overview of the Information Technology (applications and infrastructure) required to support PSO organizations, a review of industry accepted IT cost management strategies, policies, procedures and performance metrics and detailed answers to critical IT cost management questions asked by the FERC staff.

A. Project Objective

The Federal Energy Regulatory Commission and other industry stakeholders have been concerned about the ability of Power System Operators (Control Area managers, Reliability Coordinators, and Market Administrators) to control technology costs and manage large technology projects. Audits, performance reviews, and tariff filings have surfaced the issues, but attempts to develop standards, implement common practices, and create comparative performance measures have not yet satisfied these concerns.

In response to these concerns and the recognized need to take action, FERC asked Gestalt to prepare a document that summarizes technology cost management concepts and issues for an audience that includes a diverse set of power industry stakeholders. This information is intended to be used by Power System Operators (PSO) Directors, Federal and State Regulators, Grid Managers, FERC staffers and other interested industry stakeholders to help understand the cost-related impact of technology decisions.

As part of this effort, Gestalt was asked to:

- Inventory key PSO grid reliability and market management functions and the software applications used to support each function,
- Categorize and define common PSO IT cost elements,
- Outline PSO IT cost drivers, and
- Develop a set of IT performance metrics that can be used to compare IT offerings for acquisition decisions and to evaluate on-going IT operations.

In addition, Gestalt was asked to address a number of specific IT cost management questions including:

1. How should the Buy vs. Build decision be approached?
2. What PSO technologies should be considered for recycle and reuse?
3. When should applications and projects be abandoned and “sunk costs” ignored?
4. What should be considered the normal life span of PSO technologies?
5. What are the issues that arise when a limited number of vendors participate in a technology market, and how can the risks be mitigated?

6. What process can be implemented and metrics tracked to ensure that applications are being developed and operated cost effectively?
7. What is the impact of excessive delays when new technology is being implemented?
8. How cyber security concerns should be addressed in the IT acquisition and development process?

FERC requested that Gestalt prepare two deliverables for this project:

a) The first deliverable, a power point presentation summarizing the results of the effort was delivered in early July and presented at the July 14th, 2004 Software Technology Conference sponsored by FERC and held at the FERC office in Washington DC. The presentation can be found, along with the other conference presentations, on the FERC website.

b) The second deliverable, a comprehensive report detailing the work, is satisfied with the delivery of this report.

In addition to commissioning Gestalt to prepare this report, the FERC also convened a third Software Technical Conference for the PSO industry on July 14th, 2004 at the FERC office in Washington DC. Representatives from PSO organizations across the nation, along with software vendors and independent consultants, gathered to report on and discuss initiatives to increase software effectiveness, lower implementation costs, and decrease implementation timelines. After a review of the IT management principles outlined in this report, Don Watkins of the Bonneville Power Administration challenged the group to set a compelling long-term vision for the wholesale power system industry connectivity and implement a plan to get there. Don's presentation was followed by presentations from members of the ISO/RTO Information Technology Council, representatives from the Common Information Model (CIM) working group, and the EMS vendor consortium regarding initiatives to develop common architectures, data definitions, and data exchange protocols. The presentations indicated that positive progress has been made and that the FERC and other industry stakeholders should continue to support these efforts. A transcript of the conference and copies of the presentations can be found on the FERC website at www.ferc.gov

B. Project Approach

The information presented in this report was assembled by a team of PSO Industry and IT professionals from Gestalt as well as several independent technology consultants. The team developed and compiled the information based upon years of PSO and utility industry IT and operations experience. The team reviewed publicly available data and reports to verify their assumptions and test their conclusions. The team met numerous times over a two month period to discuss concepts, develop content, and edit individual results. The initial thoughts and draft documents were reviewed with several key industry stakeholders as well as with FERC staffers to ensure that the results and recommendations were clear, actionable, and realistic.

C. Report Structure

The report is structured to present background information (*Section II, III, and IV*) that can be used to support the responses to the critical questions discussed in *Section V*. *Section II* contains a fairly detailed overview of PSO functions and the technology which is used to support the performance of those functions. This information maps the technologies to the business functions

they support and provides the business context in which to understand the issues. *Section III* provides a review of IT cost management concepts and best practices which can be used to assess the cost management effectiveness of an IT organization while *Section IV* contains a review of IT performance metrics which can be used to measure and track the performance of IT organizations and technologies. *Section V* contains a review of the specific PSO technology management questions that the team was asked to address. Appendix A contains a more detailed overview of IT best practices, Appendix B provides an overview of IT risk areas and the remainder of the appendices contains detailed work products.

D. Recommendations

The body of the report provides a comprehensive overview of PSO technologies and IT management best practices and should be reviewed in detail to gain a full understanding of the technology management issues and recommendations. The key recommendations and findings include:

General Recommendations / Observations:

- As the role and responsibility of a PSO organization evolves to include Control Area management, Reliability Management, and Market Administration, significant investment in projects to develop and deploy new technology infrastructure and applications is required.
- Information Technology Governance, adherence to a defined System Development Life Cycle (SDLC) methodology, comprehensive Project Management processes, and strong vendor management practices are necessary to provide the discipline required to implement technology projects on time and within budget.
- Applications should be designed to 1) incorporate common and open architectures, protocols and platforms, 2) enable reuse, 3) ensure interoperability and 4) reduce initial and on-going support costs.
- Application implementation project costs increase disproportionately as the amount of customization increases. That is, if the amount of customization increases by 10%, the cost of the project will generally increase by an amount much larger than 10%. New application implementation costs and implementation durations can be minimized by adhering to common business practices, using standard configurations, and limiting the amount of customization.
- Industry stakeholders should continue to work together to:

- Adopt open architectures that are hardware and database independent to promote data exchange, increase interoperability.
- Adopt industry-wide information technology standards to reduce costs and increase interoperability, and extend the life span of applications.
- Develop more flexible solutions that are based upon modular designs, non-proprietary languages, use off-the-shelf software when appropriate, and positioned to leverage web services in the future.

Answers to Specific FERC Questions (more detailed responses are included in body of the report.)

Q How should the Buy vs. Build decision be approached? (see appendix V. section A for details)

No decision regarding the choice of buying a commercial "off-the-shelf" solution or building a custom-made application should be made until the business needs are well articulated and documented, user requirements are determined, and planning and analysis is completed. Any decision to build new reliability or markets applications completely from scratch, rather than re-configure or customize existing vendor products, should be scrutinized and validated. In many cases the convergence of market designs has created the ability to re-configure and customize vendor offerings at a lower cost than a complete new build.

Q What PSO technologies should be considered for recycle and reuse? (see appendix V. section B for details)

While the ability of one PSO to reuse the applications developed for another PSO is limited by a number of commercial and practical operations factors, the movement within the industry to create common architectures and data definitions will make reuse a more viable option in the future.

Q When should applications and projects be abandoned and "sunk costs" ignored? (see appendix V. section C for details)

Given the large financial outlay associated with application development projects, there is a tendency to look backwards at the sunk costs and conclude that an investment of this magnitude cannot be abandoned, regardless of the cost to complete. This is an erroneous decision making criteria, and often obscures the true viability of a project. Every project plan should incorporate cost, scope, and schedule controls and have an "exit strategy" to avoid runaway spending.

Q What should be considered the normal life span of PSO technologies? (see appendix V. section D for details)

In general, IT applications and infrastructure should not be replaced unless the business needs that they were intended to support can no longer be cost effectively met. This would include the inability to meet the functional requirements of the business, the cost to maintain the technology is significantly higher than alternatives, or the technology is obsolete and can no longer be supported.

Q What are the issues that arise when a limited number of vendors participate in a technology market, and how can the risks be mitigated? (see appendix V. section E for details)

The limited number of vendors in the Reliability Management product sector may not be an issue since the size of the market limits the number of vendors that could remain viable. However, the potential over-reliance on one or all of these vendors by a PSO may introduce risk. To mitigate the real or potential risks of a PSO dependency on one or more Reliability Management application vendors, PSO organizations should:

- Develop an applications portfolio that contains a range of Reliability Management products that fall along the "Buy vs. Build" continuum.

- Move towards an industry standard common architecture.
- Create and maintain current business/ technical requirements and design documentation of their Reliability Management functions.
- Invest in in-house technical experience with critical applications to be able to triage operations problems and facilitate and manage application modifications, interfaces and upgrades.
- Develop long-term, strategic partnerships with their critical Reliability Management application vendors that are based upon trust, shared risk/reward and mutually understood goals and objectives.

Q What process can be implemented and metrics tracked to ensure that applications are being developed and operated cost effectively? (see section III & IV for details)

The recommendations for managing on-going IT operating costs and project based development and deployment costs are based upon the use of a total cost of ownership (TCO) model of cost management. Under the total cost of ownership model, managers are required to evaluate the total expected cost of an owning and operating technology over the useful life of the application or equipment and use the total cost to compare alternative solutions, develop forecasts and create budgets.

In order to perform at a very high level, IT organizations need to institutionalize the process of measuring the performance of their organization, technology and vendors. Performance metrics should be captured in four critical areas: 1) System and Application Performance, 2) IT Service Delivery, and 3) Project Delivery, and 4) Cost.

Q What is the impact of excessive delays when new technology is being implemented? (see appendix V. section f for details)

Project delays as a result of the market and regulatory decision making process are an inevitable issue for any new PSO technology implementation. This is particularly true for those that involve new regulations, market designs, market rules, technology standards, processes and data, integration needs and organizational changes. The PSO can anticipate and manage the impact of delays by structuring the technology project into manageable releases and project phases, and by using standard Project Management and SDLC Methodologies that plan and account for critical path bottlenecks, decision making gaps. Creating a plan that uses parallel tracks may help minimize project downtime as long as the interdependencies are well known and documented.

Notwithstanding the forgoing, IT organizations can not be expected to implement complex software designed to support reliability or market operations without completing a significant amount of detailed business process and rules development work. Vague, unclear or unfinished business rules inevitably lead to stalled projects and delayed implementations. Software may not be configured and customized to support specific design permutations until the basic design decisions are made. The result of repeated design changes or stalled decision making is costly overruns and embarrassing implementation delays. Project teams on large projects can easily reach 100 or more members where delays can easily cost $1 million or more per month.

Q How should cyber security concerns be addressed in the IT acquisition and development process? (see appendix V. section G for details)

Determine the hardware and software security requirements and design security features at the beginning of the project to ensure that cyber security is integrated throughout the entire system and not treated as after-thoughts.

Understand and comply with NERC Standard 1200 and include consideration of the standards in the specification setting and alternative analysis setting processes.

- NERC Standard 1200 adopted August 2003 and extended through August 13, 2005 to "reduce risks to the reliability of the bulk electric systems from any compromise of critical cyber assets"
- Mandatory compliance with Standard 1200 by 1Q2005 is required for those entities under FERC oversight
- The anticipated permanent Standard 1300 will have fines and penalties for non-compliance.

III. Power System Operations Functions

A. Section Summary:

In this section the information technology, both applications and infrastructure, required to support power system operations organizations is defined, described and linked to the business processes and functions it supports.

Gestalt was asked to provide technology guidelines that could be used to evaluate the reasonableness of a Power System Operator's (PSO) proposed cost of operations. The specific business model that is in place for the PSO heavily influences the technology requirements. Thus, any evaluation of the proposed cost of operations needs to be done in light of the business model. This section documents the spectrum of potential PSO business models and the technology that is deployed to support each model. These business models are developed utilizing three basic building blocks: Control Area functions, Reliability Coordinator functions and Market Operator functions. The technology guidelines that are discussed throughout the remainder of this document are done within this context of potential PSO business models. The three basic PSO models are presented in an evolutionary manner, moving from a PSO with Reliability Coordination only functionality to a PSO that performs Reliability Coordination, Control Area functions and Market Administration. In addition to the three PSO models, we have included an Autonomous Control Area model to represent the fact that many Control Areas are not currently members of an existing ISO or RTO.

After defining the various PSO Business Models, the functions preformed by PSO organizations operating under the four models are defined and the technology required to support them is detailed. The functions are divided into the nine business process areas listed below. Figures 3 through 12 in this section provide a graphical summary of the software and applications typically used to support each functional area.

1. Transmission Grid Security
2. Transmission Expansion Planning
3. Scheduling Operations
4. Real Time Operations
5. Market Administration
6. Customer Service Processes
7. Payroll & HR Functions
8. Finance and General Accounting
9. Corporate Administration

The section ends with a summary of the technology infrastructure elements (computer hardware and communications equipment) required to support PSO operations. As would be expected the technology investment required to support the various functions of the PSO organization increases as the business moves through the four evolutionary models.

B. PSO Business Models

The specific business model that is in place for the PSO heavily influences the technology requirements. Thus, any evaluation of the proposed cost of operations needs to be done in light of the business model. This section documents the spectrum of potential PSO business models. These business models are developed utilizing three basic building blocks: Control Area functions, Reliability Coordinator functions and Market Operator functions. The technology guidelines that are discussed throughout the remainder of this document are done within this context of potential PSO business models. The three basic PSO models are presented in an evolutionary manner, moving from a PSO with Reliability Coordination only functionality to a PSO that performs Reliability Coordination, Control Area functions and Market Administration. In addition to the three PSO models, we have included an Autonomous Control Area model to represent the fact that many Control Areas are not currently members of an existing ISO or RTO. These Control Areas will ultimately need to make the choice of becoming a new PSO or joining an existing PSO. If the Control Area ultimately becomes a new PSO, it will likely follow the evolutionary path described above. Alternatively, the Control Area could join an existing PSO and either retain its Control Area status or allow the PSO to perform Control Area functions on its behalf. The Control Area model and the three PSO models can be summarized as follows and are depicted below in Figure 1. Each model is discussed in further detail in the following sections.

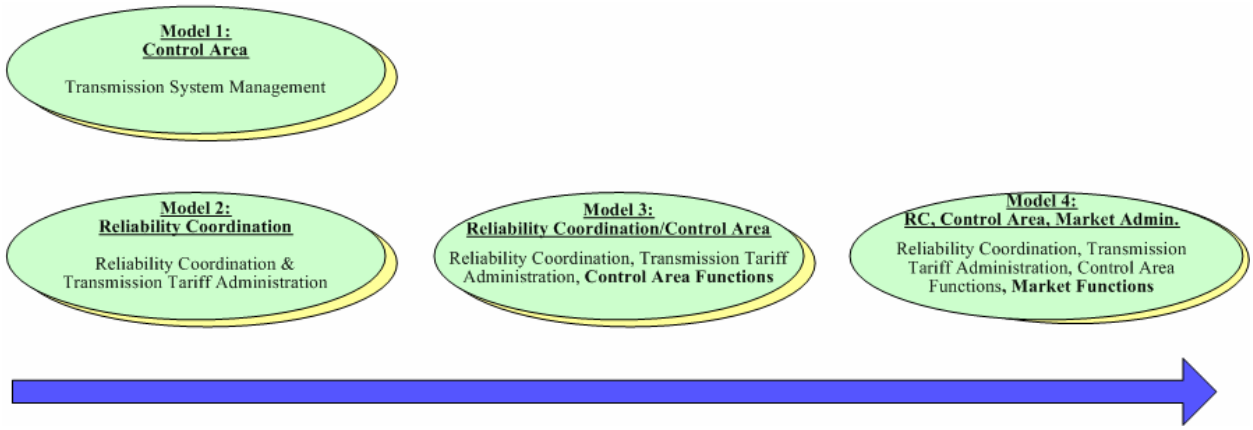
Model 1: Autonomous Control Area with open access provided via 888 Tariff

Model 2: Power System Operator with Reliability Coordination Functions

Model 3: Power System Operator with Reliability Coordination and Control Area Functions

Model 4: Power System Operator with Reliability Coordination, Control Area and Market Administration functions.

a. Figure 1 – Power System Operator Business Models



As a PSO moves along this continuum, its responsibilities obviously increase. Concomitantly, the costs associated with providing the technology services also increases. Figure 2 depicts this conceptual relationship between the cost and complexity of PSO operations as the PSO's responsibility increases through the addition of greater functionality. A significant amount of technical related costs are incurred in the transition to Model 2 to ensure that the PSO can meet its Reliability Coordinator responsibilities. These costs are primarily driven by the need to

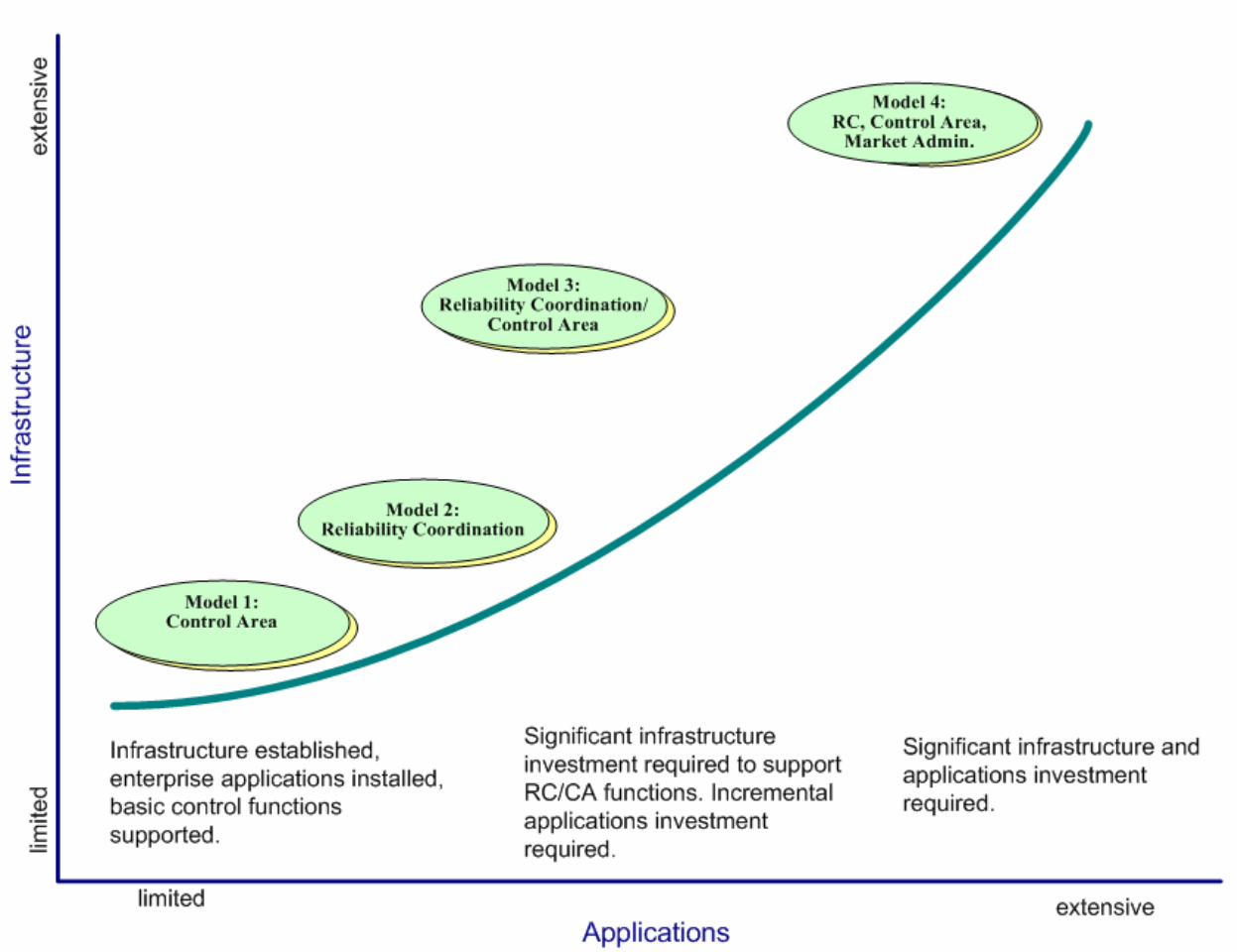
install and maintain an Energy Management System (EMS) that provides the PSO with real-time transmission system monitoring and analysis capabilities that the PSO requires for managing transmission congestion including the implementation of transaction curtailment procedures (NERC TLR) on a regional basis.

Under Model 3, the PSO incrementally increases its responsibilities by adding Control Area operation functionality. Typically, the PSO would add this responsibility through the consolidation of Control Areas under the PSO's footprint and the desire of the Control Area operators of the consolidated Control Areas to have the PSO perform this function. Typically, the incremental cost to the PSO to perform this added function is relatively small as compared to Model 2 costs. AGC and frequency control functions are typically included within an EMS system so the costs to the PSO will be limited to the implementation of an existing EMS application. Additionally, the PSO would typically perform economic dispatch functions for the former Control Area operator that would create the need for the addition of a security constrained economic dispatch (SCED) application within the EMS. However, there could be significant cost reductions to the former Control Area operators because they no longer need to maintain or replace significant portions of their EMS systems (some EMS functionality will remain for the management of the distribution system).

The PSO's cost increases in its transition to Model 4 will be more significant than the costs associated with moving from Model 2 to Model 3. The application and infrastructure foundation implemented in the earlier phases can be leveraged but the new functions introduced at this time will generally result in considerable expenditures. The major cost drivers under Model 4 will be the additional EMS applications required for operation settlement of the day-ahead and real-time energy markets. For a Locational Marginal Pricing (LMP) based congestion management system, these additional applications would include Financial Transmission Rights (FTR), Simultaneous Feasibility Test (SFT) and FTR market clearing software. The amount of the cost increase will depend upon the market functionality added. For example, if the RTO is already performing SCED, the addition of real-time energy market functionality would require the addition of LMP calculations to the Model 2 SCED application. This cost would be relatively small as compared to adding additional applications and business functions for day-ahead market operations and ancillary service market operations and the associated multi-settlement systems that would be required.

The relationship between PSO functionality and required infrastructure and applications is depicted in Figure 2. Figure 2 shows the basic building block functions starting with Control Area functions and then adding Reliability Coordination and Market Administration functions. As functionality is added, more applications and infrastructure are required. The addition of the Market Administration functions requires a significant increase in infrastructure and applications as compared to those required for Reliability based functions.

b. Figure 2 – Relationship between PSO Functions/Responsibility & Complexity/Cost



C. Model 1 – Autonomous Control Area (see Appendix VIII)

We have included this scenario in order to represent existing conditions in the Pacific Northwest and Southeastern regions of the US. Although, discussions about forming RTO organizations have been underway for many years (e.g. Grid West, SETRANS, GridFlorida) within these regions, agreement to move forward with implementation has not yet been reached. Therefore, a significant number of Control Areas exist that continue to operate under their Order 888 Open Access Transmission Tariffs (OATT). Each of these Control Areas basically performs the functions as listed under RTO Model 3 below but on a smaller, sub-regional scale. The diagram in Appendix B demonstrates the major functions that are provided by a Control Area.[3] The key operating characteristics associated with a Control Area are as follows:

- The Control Area administers an Order 888 OATT and provides transmission service within the Control Area boundaries.

[3] It is assumed that the transmission owner is the Control Area operator and that this service has been functionally unbundled from other transmission business operations.

- The Control Area is responsible for operating and maintaining an OASIS node on behalf of transmission owners with the Control Area boundary.
- The Control Area may or may not be the NERC Reliability Coordinator. For example, in the Pacific Northwest, the Pacific Northwest Security Coordinator (PNSC), which is not a Control Area, performs the Reliability Coordination function for 15 controls areas within the Pacific Northwest region. Conversely, Entergy, PJM the New York ISO and ISO New England are all Reliability Coordinators that are also Control Areas.
- The Control Area does not administer any energy or ancillary service markets; only administration of the schedules included in the OATT is performed.
- The Control Area manages internal and external energy transaction schedules.
- The Control Area provides balancing energy and operating reserves. Balancing energy here amounts to inadvertent energy and is managed via AGC and Economic Dispatch. The Control Area is also responsible for maintaining system frequency, managing net-tie schedules, inadvertent energy tracking and payback and adherence to CPS1 and CPS2 NERC system control criteria.

D. Model 2 - PSO with Reliability Coordination (see Appendix IX)

Under this scenario, the PSO is charged with providing Reliability Coordination services for the Control Areas within its footprint. The diagram in Appendix B demonstrates the major functions that are provided by the PSO under Model 2; it also shows the division of responsibilities between the PSO and Control Area Operators/Local Control Centers. The key operating characteristics associated with Model 2 are as follows:

- The PSO administers a region-wide transmission tariff and provides transmission service.
- The PSO is responsible for operating and maintaining a region-wide OASIS node.
- The PSO is the NERC Reliability Coordinator.
- The PSO is not a Control Area Operator.
- The PSO does not administer any energy or ancillary service markets.
- Transaction schedules between Control Areas (both internal and external to the PSO) are managed by the PSO.
- Control Area services (e.g. AGC, Frequency Response, adherence to CPS1 and CPS2 NERC system control criteria) are provided by existing Control Areas.
- Balancing energy and operating reserves provided by the PSO via agreements with existing Control Areas. Balancing energy here amounts to inadvertent energy and is managed via AGC and Economic Dispatch.

E. Model 3 - PSO with Reliability Coordination and Control Area Functions (see Appendix X)

Under this scenario, the PSO is charged with providing Reliability Coordination in addition to Control Area functions. Appendix C reflects the major PSO functions under Model 3 and shows

the division of responsibilities between the PSO and Control Area Operators/Local Control Centers. The key operating characteristics associated with Model 3 are as follows. Changes in functionality from Model 2 are shown in bold.

- The PSO administers a region-wide transmission tariff and provides transmission service.
- The PSO is responsible for operating and maintaining a region-wide OASIS node.
- The PSO is the NERC Reliability Coordinator.
- The PSO is a Control Area Operator.
- The PSO does not administer any energy or ancillary service markets.
- Transaction schedules between Control Areas (both internal to PSO and external) are managed by the PSO.
- The PSO will perform hierarchical Control Area coordination within the PSO footprint.
- Control Area services may be provided by the PSO or a combination of the PSO and any remaining Control Areas under the PSO's footprint (AGC, Frequency Response, adherence to CPS1 and CPS2 NERC system control criteria).
- Balancing energy and operating reserves provided by the PSO via agreements with existing Control Areas. Balancing energy here amounts to inadvertent energy and is managed via AGC and Economic Dispatch. **For PSO operated Control Areas, the PSO will perform economic dispatch function along with the AGC function to maintain net tie schedules and system frequency.**

F. Model 4 - PSO with Reliability Coordination, Control Area Functions and Market Administration (see Appendix XI)

Under this scenario, the PSO is charged with providing Reliability Coordination, Control Area, and Market Administration functions. Appendix D shows the major PSO Functions under Model 4 and shows the division of responsibilities between the PSO and Control Area Operators/Local Control Centers. The key operating characteristics associated with Model 4 are as follows. Changes in functionality from Model 3 are shown in bold.

- The RTO administers a region-wide transmission tariff and provides transmission service.
- The RTO is responsible for operating and maintaining a region-wide OASIS node
- The RTO is the NERC Reliability Coordinator.
- The RTO is a Control Area Operator and maintains hierarchical control over the RTO footprint.[4]

[4] Hierarchical control is required if one or more systems under the RTO footprint maintain their Control Area status and the RTO is also a Control Area operator. Typically, dynamic scheduling capabilities will be required by the RTO to accomplish this coordination such that RTO's operation of the system appears to be equivalent to a single Control Area operation.

- The RTO administers RTO-wide energy or ancillary service markets which may potentially include:
  - **An LMP based congestion management system with FTR markets**
  - **A binding day-ahead energy market**
  - **A real-time energy market for balancing energy**
  - **Ancillary service markets for AGC, spinning reserve and non-spinning reserve**
  - **Installed capacity obligations and associated markets**
- Transaction schedules external to the RTO footprint are managed by RTO. The RTO may continue to manage internal schedules between Control Areas via dynamically scheduling. Dynamic scheduling between Control Areas within the RTO footprint is required in order to maintain an RTO-wide real-time energy market.
- The RTO will perform hierarchical Control Area coordination within the RTO footprint.
- Control Area services (AGC, Frequency Response, adherence to CPS1 and CPS2 NERC system control criteria) may be provided by the RTO or a combination of the RTO and any remaining Control Areas under the RTO's footprint.
- Balancing energy and operating reserves provided by the RTO via market mechanisms. The RTO performs a system-wide security constrained economic dispatch and communicates dispatch instructions via local control centers or directly to generating units.

G. Power Systems Operators Business Processes/Functions

The following sections describe the functions that are performed by the PSOs and graphically depict how the functions change based upon the PSO model that is in effect.

1. Transmission Grid Security

Transmission Grid Security Processes/Functions are generally performed by the System Operations organization and include those processes required to monitor and manage the transmission system. A description of these major processes is included in Figure 3.

a. Figure 3 – Transmission Grid Security Processes

Responsible Org: System Operations							
BP #	Transmission Grid Security	Category	Description	Control Area	Reliability Coordinator	Reliability Coordinator & Control Area	RC, CA & Market Operator
TG1	Calculate / Update TTC	Reliability	Update transmission system total transfer capability based upon current and forecasted system conditions.				
TG2	Monitor and Maintain System Security	Reliability	Monitor system conditions via contingency analysis and performance of NERC Security Coordinator role.				
TG3	Manage System Restoration	Reliability	Develop/maintain system restoration plans and implement when needed.				
TG4	Provide Outage Coordination	Reliability	Provide final approval of requested transmission outages and coordinate with generation outages				
TG5	Calculate Ancillary Service Requirements	Reliability	Calculate Regulation, Operating Reserve and Black Start requirements.				
TG6	Provide Operator Training	Reliability	Provide system operator training via training simulator.				
TG7	Develop and Maintain Procedures	Reliability	Develop/maintain system operating procedures and standards, including creation of training protocols.				

Key	Primary	Significant	Modest	Minor	None

2. Transmission Expansion Planning

Transmission Expansion Planning Processes/Functions are generally performed by the System Planning organization and include those processes required to plan additions and enhancements to the transmission system so that it will be sufficient to deliver generation to load in the future. A description of these major processed is included in Figure 4.

a. Figure 4 – Transmission Expansion Planning Processes

Responsible Org: System Planning							
BP #	Transmission Expansion Planning	Category	Description	Control Area	Reliability Coordinator	Reliability Coordinator & Control Area	RC, CA & Market Operator
TP1	Perform Long Range Planning	Reliability	Perform studies to assess future state of transmission system and recommend enhancements to maintain required level of reliability.				
TP2	Evaluate Long-Term Transmission Service Requests	Reliability	Perform studies in response to requests for long-term transmission service to determine if any system enhancements are required.				
TP3	Evaluate Generator Interconnection Requests	Reliability	Develop interconnection standards and evaluate new generator interconnection requests to determine system enhancements required.				

Key: Primary | Significant | Modest | Minor | None

3. Scheduling Operations

Scheduling Operations Processes/Functions are generally performed by the System Operations organization and include those processes required to develop a reliable operating plan for next day operations such that sufficient generation and transactions are scheduled to meet forecasted energy and ancillary service requirements. A description of these major processes is included in Figure 5.

a. Figure 5 – Scheduling Operations Processes

Responsible Org: System Operations				Control Area	Reliability Coordinator	Reliability Coordinator & Control Area	RC, CA & Market Operator
BP #	Scheduling Operations	Category	Description				
SO1	Receive Bid Data	Markets	Collect and store generator offers and load bids for future use in scheduling and dispatching the system.				Primary
SO2	Forecast System Load	Reliability	Provide forecasts of real-time hourly peak loads for each hour on a day-ahead basis	None	Minor	Modest	Primary
SO3	Schedule generation and ancillary services	Reliability	Perform Security Constrained Unit Commitment to ensure that sufficient capacity is committed for the next day to meet forecasted energy/ancillary service requirements.	Primary	None	Modest	Primary
SO4	Calculate/Update Available Transmission Capacity (ATC).	Reliability	Modify TTC to account for confirmed transaction schedules	Significant	Primary	Primary	Primary

Key: Primary | Significant | Modest | Minor | None

4. Real-Time Operations

Real-Time Operations Processes/Functions are generally performed by the System Operations organization and include those processes required to maintain moment-to-moment generation and load balance and to maintain system security. A description of these major processes is included in Figure 6.

a. Figure 6 – Real-Time Operations Processes

Responsible Org: System Operations				Control Area	Reliability Coordinator	Reliability Coordinator & Control Area	RC, CA & Market Operator
BP #	**Real-Time Operations**	**Category**	**Description**				
RT1	Monitor Trans. Grid and Dispatch Generation	Reliability	Dispatch generation on a minute-to-minute basis to maintain generation/load balance taking into account real-time status of system.				
RT2	Manage Congestion	Reliability	Ensure real-time energy dispatch is performed so transmission elements can be operated within normal limits following a single contingency.				
RT3	Dispatch Ancillary Services	Reliability	Dispatch regulation and operating reserves as needed.				
RT4	Implement Emergency Procedures	Reliability	Execute external transaction curtailment priority and curtailment.				
RT5	Monitor Compliance with Dispatch Orders	Reliability	Track and record generator actual energy output and compare to compliance rules				
RT6	Collect Interchange Meter Data	Markets	Collect and record data for later use in Settlements				

Key	Primary	Significant	Modest	Minor	None

5. Market Administration

Market Administration Processes/Functions are generally performed by the Market Operations organization to ensure the proper and efficient functioning of the energy and ancillary services markets and include those processes required to operate and settle energy and ancillary services markets. These functions include OASIS operations, Day-Ahead and Real-Time Market operations, Credit, Settlements, and Market Monitoring. A description of these major processes is included in Figure 7.

a. Figure 7 – Market Administration Processes

Responsible Org: Market Operations

BP #	Market Administration	Category	Description	Control Area	Reliability Coordinator	Reliability Coordinator & Control Area	RC, CA & Market Operator
MA1	Maintain OASIS Node	Reliability	Operate OASIS Node for RTO Region.				
MA2	Manage Transmission Services	Markets	Receive, validate and approve/deny short-term transmission reservation requests via OASIS.				
MA3	Operate Day-Ahead Market	Markets	Create binding day-ahead market schedule and binding day-ahead market prices utilizing security constrained unit commitment and economic dispatch tools.				
MA4	Procure Ancillary Services	Markets	Potentially operate markets for: Regulation, Operating Reserve (10 min spin, 10 min non-spin, 30 min), Installed Capacity.				
MA5	Operate Congestion Mgt Market	Markets	Potential operate auction market for Financial Transmission Rights (FTRs)				
MA6	Operate Real-Time Balancing Market	Markets	Calculate real-time balancing energy prices.				
MA7	Certify Meters	Markets	Certify and register meters and maintain approved meter database.				
MA8	Certify New Customers	Markets	Gather customer information for customer participation in RTO activities and certify customer has met requirements				
MA9	Acquire real-time metering data	Markets	Receive, validate and store revenue quality metering data for generation and load.				
MA10	Settle the markets	Markets	Calculate charges/credits for Ancillary Services, balancing energy (accounting for day-ahead market if any), and FTRs.				
MA11	Administer Transmission Tariff	Markets	Calculate transmission charges/credits and remaining non-market related ancillary service schedules.				
MA12	Perform Billing	Markets	Prepare billing invoices and render bills to participants (Monthly/weekly/daily).				
MA13	Manage Credit Risk	Markets	Estimate customer charges on an on-going basis and ensure that total estimated charges do not exceed customers credit limit.				
MA14	Resolve Billing Disputes	Markets	Collect pertinent data required associated with dispute and follow dispute resolution process as defined in rules/tariff.				
MA15	Receive and Disperse funds	Markets	Coordinate collection and disbursement of cash, monitor and track outstanding amounts and enforce collection procedures.				
MA16	Market Monitoring	Markets	Monitor market activity and results and modify rules to correct flaws and/or to address market power issues.				

Key	Primary	Significant	Modest	Minor	None

6. Customer Service

Customer Service Processes/Functions are generally performed by the Customer Service organization to manage the customer interface. They include those processes to provide customer training and to ensure that customer related problems, issues, and requests are dealt with in a timely and efficient manner. The introduction of an energy and ancillary services markets significantly increases the importance of these functions. A description of these major processes is included in Figure 8.

a. Figure 8 – Customer Service Processes

Responsible Org: Customer Service								
BP #	Customer Service	Category	Description	Control Area	Reliability Coordinator	Reliability Coordinator & Control Area	RC, CA & Market Operator
CS1	Respond to customer inquiries	Corporate	Obtain answers to customer questions. Act as single point of contact between RTO and customers. Maintain database of customer info.				
CS2	Disseminate information to customers	Corporate	Provide info on transmission system, settlement, billing, markets and other relevant info.				
CS3	Provide Customer Training	Corporate	Design, develop and deliver customer training.				

Key: Primary | Significant | Modest | Minor | None

7. Payroll & Human Resources

Payroll and Human Resources Processes/Functions are generally performed by the Corporate Service organization to address the internal needs related to managing the PSO work force. They include those processes required for managing internal human resources including training, compensation and benefits. These functions are not significantly affected by the business model in which the PSO is operating. A description of these major processes is included in Figure 9.

a. Figure 9 – Payroll & HR Processes

Responsible Org: Corporate Services				Control Area	Reliability Coordinator	Reliability Coordinator & Control Area	RC, CA & Market Operator
BP #	**Payroll & HR**	**Category**	**Description**				
PH1	Execute Payroll & Time/Expense Reporting	Corporate	Calculate payroll and perform corresponding tax reporting functions				
PH2	Manage Human Resources	Corporate	Develop, implement and maintain HR policies and procedures. Recruit employees. Manage employee and organizational development.				
PH3	Manage Benefits	Corporate	Develop, implement and maintain benefit policies, procedures and plans.				
PH4	Manage Training Needs	Corporate	Define and plan customer and employee training needs.				

Key: Primary | Significant | Modest | Minor | None

8. Finance & General Accounting

Finance and General Accounting Processes/Functions are generally performed by the Corporate Service organization to enable the PSOs to meet their fiduciary duty of managing their expenditures. They include those processes required to manage all financial aspects of the organization. These functions are not significantly affected by the business model in which the PSO is operating. A description of these major processes is included in Figure 10.

a. Figure 10 – Finance & General Accounting Processes

Responsible Org: Corporate Services				Control Area	Reliability Coordinator	Reliability Coordinator & Control Area	RC, CA & Market Operator
BP #	Finance & General Accounting	Category	Description				
FG1	Perform Financial Management & Accounting	Corporate	General Ledger, Accounts Receivable, Accounts Payable, Fixed Assets, FERC uniform system of accounts, financial risk management.				
FG2	Manage Capital	Corporate	Management of RTO capital spending including: development of capital mgt processes, structure, budgets, and prioritization of projects.				

Key: Primary | Significant | Modest | Minor | None

9. Corporate Administration

Corporate Administration Processes/Functions are generally performed by the Corporate Service organization to manage and monitor the organization's processes and ensure that it is accomplishing its goals in an efficient and effective manner. The introduction of an energy and ancillary services markets significantly increases the importance of several of these functions. A description of these major processes is included in Figure 11.

a. Figure 11 – Corporate Administration Processes

Responsible Org: Corporate Services							
BP #	**Corporate Administration**	**Category**	**Description**	**Control Area**	**Reliability Coordinator**	**Reliability Coordinator & Control Area**	**RC, CA & Market Operator**
CA1	Strategic Planning & Performance	Corporate	Development of RTO long term vision and strategy including defining RTO mission, core values and culture.				
CA2	Manage Security	Corporate	Define, implement and manage security access controls and physical security of facilities.				
CA3	Develop Corporate Communications	Corporate	Develop internal and external corporate communication policies. Manage internal and external communications.				
CA4	Perform Audits	Corporate	Perform Internal Auditing				
CA5	Manage Facilities and Purchasing	Corporate	Responsible for management and maintenance of RTO facilities and purchasing decisions.				
CA6	Provide Legal Support	Corporate	Provision of legal services including support of Tariff and rule changes.				
CA7	Interface with regulatory bodies	Corporate	Communications with regulatory bodies and monitoring regulatory developments.				
CA8	Manage Business Information Technology	Corporate	Provide IT strategy to support business related systems (not control systems associated with system operation)				

Key	Primary	Significant	Modest	Minor	None

H. PSO Applications

In order to perform the processes and functions listed in the previous sections, the PSOs rely upon a set of major applications that are fairly standard across the industry. These applications are often procured from independent software vendors, though in some cases the applications have been developed for the PSO by its own development staff or by software development vendors contracted specifically to develop the application.

Figure 12 provides a listing and description of the typical applications that are used and the function that they provide. Generally, the applications can be grouped into three major categories: Reliability Coordination, Market Administration and Corporate applications. Major applications under Reliability include: Energy Management System (EMS) that is required to monitor real-time transmission system flows and voltages and for generation and load balancing; both SCUC and SCED applications without market clearing algorithms for scheduling and dispatch; and network analysis tools such that contingency analysis can be performed to ensure that the system can be operated reliably under single contingency outage conditions. A PSO that is both a Control Area operator and Reliability Coordinator would need to acquire all of the reliability-based applications listed in Figure 12. The reliability applications are fairly mature as the fundamental engineering calculations and algorithms have been in place for many years. The challenge that they are currently facing is one of human factors and data presentation. These applications will need to become more adept at processing large amounts of data, analyzing, interpreting, and presenting it to the operator in a manner that is understandable and actionable.

A PSO that is serving as a Market Administrator would need to include the market applications in addition to the applications required for Reliability Coordination. Major applications under Market Administration include: Security Constrained Unit Commitment (SCUC) that is used for day-ahead scheduling and clearing of the day-ahead markets; Security Constrained Economic Dispatch (SCED) that is used for generation dispatching and real-time market clearing; and market settlement systems that calculate market participant charges and credits associated with the day-ahead and real-time markets. The market applications build on the reliability applications foundation, and thus, need to be tightly integrated with the reliability applications. These applications are generally less mature and will undergo significant change over the next few years. Corporate applications are generally required by Control Area operators and all three PSO models.

As a PSO assumes more functional responsibility, it needs to initiate major projects to implement the applications that enable it to perform the processes and functions shown in Section II F 1 through Section II F 9. For example, before the PSO begins to assume the responsibility for administering an energy market, it must have captured the requirements for, architected, designed, constructed, and tested the applications in the “Market Applications” category. Appendices G and H depict the applications relevance for the PSOs based upon the model within which it is operating.

a. Figure 12 – PSO Applications & Descriptions

FERC IT Guidelines Project - ISO/RTO Applications			
	Appl#	**Application Name**	**Function**
Open Access Transmission Service Applications	A01	External Transaction Scheduler	Used to schedule external transactions, including through and out transactions.
	A02	Open Access Same Time Information System	Management of transmission service requests
	A03	Total Transfer Capability (TTC) Calculator	Analysis package that calculates transmission system import/export capability between control areas.
	A04	Available Transfer Capability (ATC)	Analysis package that adjusts TTC to account for confirmed transmission reservations.
	A05	Transmission Tariff Settlement System	Calculation of Tariff charges/credits
Market Applications	A06	Participant Bidding System	Offer/Bid processing including submission of internal bilateral transactions (financial schedules);
	A07	Day-Ahead SCUC/SCED - LMP	Security Constrained Day-Ahead unit commitment and economic dispatch with LMP market clearing calculations.
	A08	Real-Time SCED - LMP	Generate dispatch instructions on a 5 minute basis utilizing security constrained Optimal Power Flow (OPF). Calculate real-time LMPs.
	A09	FTR Auction System	FTR Auctions, Simultaneous Feasibility Test system.
	A10	Ancillary Service Auction System	Market clearing for regulation, operating reserves, installed capacity
	A11	Customer Service, Credit & Registration	Customer service, asset registration & credit management systems
	A12	Billing System	Invoicing and Funds transfer. Daily/weekly/ monthly billing system
	A13	Market Settlement	Commercial model, settlement calculations
	A14	Meter Data Acquisition	Data acquisition, verification and error reporting.
Short-Term Transmission System Reliability Applications	A15	Energy Management System (EMS)	SCADA system, State estimator, Network Model, AGC, VAR/voltage control, Reserve Monitor (real and reactive).
	A16	Dynamic Scheduling System	System that enables the calculation of dynamic schedules for use by control areas under the RTO footprint. Requires RTO EMS to CA EMS link to update tie-schedules such that updated CA tie schedules are included in ACE calculation.
	A17	Day Ahead SCUC/SCED	Security constrained unit commitment and reliability assessment tool. Need to perform Security Coordination duties. Market clearing function not included.
	A18	Network Analysis Package	Contingency Analysis, Optimal Power Flow, Stability Analysis. Includes power flow for use in study mode.
	A19	Real-Time security constrained economic dispatch.	Generate dispatch instructions on a 5 minute basis utilizing security constrained Optimal Power Flow (OPF).
	A20	RCIS	Reliability Coordinator Information System - allows for easy transfer of data between Reliability Coordinators. Provides input to IDC.
	A21	Interchange Distribution Calculator (IDC)	Automatically calculates transaction flow distribution on monitoring transmission interface. Needed for implementation of NERC TLR procedures.
	A22	Outage Scheduler	Coordinate generation and transmission planned outages and record and track generator forced outages
	A23	Load Forecasting	Load forecasting suite with integrated weather forecast inputs.
	A24	Dispatcher Training Simulator (DTS)	Redundant EMS for use in training system operators.
Market Monitoring	A25	IMM	Independent market monitoring and mitigation
Trans Plan	A26	Transmission Planning Analysis Suite	Long Term load forecasting, power flow (PSSE), stability analysis, short circuit analysis.
Corporate Admin. Applications	A27	Compensation & Benefits	Payroll & Benefits software
	A28	Human Resources	HR System
	A29	Customer Information	Customer Information and Relationship management
	A30	Accounting	Accounting System including: GL, Accounts Receivable/Payable, fixed assets, treasury, purchasing, budgeting, time reporting.

I. PSO Infrastructure

As described in the previous section, the importance of the PSO's applications to sustain and improve its operations is usually clearly understood. However, the necessary infrastructure technologies that support these applications can be somewhat of a mystery. Mainframe systems and server farms that house the required applications all have unique and costly infrastructure that support the transfer and processing of operations data. There is also a need to capture, process, and store data from Remote Terminal Units in the field making it available to the applications that require it. In addition, to properly manage the applications, multiple instances of the infrastructure generally need to be maintained so that the production environment is properly shielded from development and test activities. A disaster recovery site that contains duplicative instances of the infrastructure is required in the event that the primary data center is rendered unusable by catastrophic events.

Other infrastructure elements (e.g. phone systems, desktops) provide other technology services to end users that have become indispensable to their performing their business processes and functions. The following infrastructure components define the technology baseline that is used to support the application and SCADA environments. It is an area that is most often overlooked from a cost and technology perspective. PSOs are eager to track key performance indicators related to application and server environments, but often ignore the foundation that supports this equipment. It is imperative that refresh, maintenance, processes and strategy are an integral part of each of these platforms, because without the proper care and feeding, the risks could be extensive. Appendix I provides further information regarding the infrastructure that is required to support the various business functions.

1. Mainframe / Servers

Mainframes and servers provide computing processing capacity for applications to run. Multiple small applications can run on the same server while large mission critical applications generally require multiple servers to improve reliability.

2. Storage Systems

Storage systems are used for information storage and retrieval by applications and end users. They are integrated with the mainframe and server environments. Specialized storage architecture (SAN/Network Attached, etc.) allow access from multiple servers and allow for a higher level of performance and reliability.

3. Routers (Wide Area Network) and Switches (Local Area Network)

Routers and switches are network equipment that is required for supporting LAN and WAN environments. Servers and workstations are located on LAN's while multiple locations are connected with WAN's.

A router is a device which forwards data packets between at least two Local Area Networks (LANs) or Wide Area Networks (WANs) based upon software-assigned addresses (e.g., an IP Address in IP-based networks). Routers, typically located at the gateway between separate networks, are designed to interrogate information contained in packet headers and determine the optimal path for forwarding the packets based on distance, cost algorithms, and user administrable criteria.

A switch is a device that filters and forwards incoming data packets from multiple input ports between Local Area Network (LAN) segments to the specific output port that will take the data packet toward its intended destination. A switch determines which output port to forward data from the physical device (Media Access Control or MAC) address in each incoming message frame.

4. Remote Terminal Units (RTU)

Remote Terminal Units (RTU) are hardware devices located in the field whose function is to monitor and control process equipment at remote locations, acquire data from the equipment and transfer the data back to the central SCADA system. These devices may be owned by the PSO, by the Control Area operator, or by transmission owners.

5. Network Circuits

Network circuits are leased from telecommunications' carriers and are used for supporting WAN's, RTU's, and for providing voice services. Circuit choices are dependent on the termination equipment, defined speed, and redundancy requirements (i.e. RTU, Server Farm, Disaster Recovery, etc.).

6. Network / Systems Management

Network and Systems Management equipment are ISO FCAPS (International Organization for Standards/Fault, Configuration, Accounting, Performance and Security) defined layers of hardware and software tools to resolve problems, configure, alarm and track the installed base of equipment.

7. Network Operations Center / Help Desk Tools

Network Operating Centers and Help Desk tools allow IT organizations to monitor and manage the equipment and computing environments.

8. Network Tools / Network Security

Network tools support problem analysis, performance trending analysis, and capacity planning to manage the infrastructure environment into which they are integrated. Network Security tools (e.g. network intrusion) help the organization manage the network to ensure that no unauthorized access or tampering occurs.

9. Laptops / Desktops

Laptops and Desktops are Personal Area Network equipment (desktop/laptop PC, palm devices, etc.) that provide access to applications and support personal productivity applications (Email, Calendaring, word processing).

10. PBX / Centrex / Voicemail

Private Branch Exchanges (PBX) and Centrex environments contribute to solid voice communications with integrated designs. Voicemail systems enable voice recordings and delivery of voice messages.

11. Turret Consoles

Turret systems are specialized voice systems that are generally utilized in Operations Centers and are integrated into dispatcher consoles.

12. VOIP

Voice Over IP (VOIP) is a specialized technology that migrates analog/voice platforms to an IP-centric system allowing voice and data transmission across a common network.

13. Wireless LAN

There are multiple wireless platforms that extend from Local Area Networking to licensed frequencies that supporting Microwave and/or SCADA RTU platforms.

14. Internet Connectivity / Remote Connectivity

Internet connectivity equipment provides connections for the corporate network to the Internet through Telecommunications links. Remote connectivity allows authorized personnel to access the network and its applications from remote locations in a secure manner.

15. Disaster Recovery

Disaster Recovery sites are duplicate data center environments that enable an organization to continue to run its applications and provide technology based services in the event that its primary data center is rendered unavailable. Similar equipment needs to be procured and installed, the applications need to be loaded, and the data needs to be copied on at least a daily basis in order for the disaster recovery site to be useful.

IV. IT Cost Management Best Practices

A. Section Summary:

In this section the policies, processes, and procedures considered most effective for managing the cost to deploy, operate and maintain IT applications and infrastructure are discussed. The policies, processes and procedures are referred to as "best practices" because they are the techniques employed by organizations generally considered the most effective at managing and controlling IT costs.

The recommendations for managing on-going IT operating costs and project based development and deployment costs are based upon the use of a total cost of ownership (TCO) model of cost management. Under the total cost of ownership model, managers are required to evaluate the total expected cost of an owning and operating technology over the useful life of the application or equipment and use the total cost to compare alternative solutions, develop forecasts and create budgets.

Recommendations associated with managing annual IT operating costs include:

- Employ organization-wide technology standards for architecture, hardware, software, operating systems, databases, and protocols to minimize development, maintenance, and support costs. Common and open architectures, protocols and platforms enable reuse, ensure interoperability and reduce costs.
- Maintain up-to-date policies, procedures, guidelines and configuration documentation to minimize maintenance and replacement costs.
- Employ release management, refresh, and retirement strategies to manage total life cycle costs.
- Employ supply and contract management strategies to maintain checks and balances with vendors.
- Track, trend, and analyze usage and cost data to identify cost management opportunities.
- Provide user organizations with usage and cost data to enable frontline cost management.
- Maintain an accurate asset database and link it to warranty, license, maintenance and support agreement information.

Recommendations associated with managing project based technology costs include:

- Build flexibility into the design. Reliability policies and rules will change over time and applications must be able to easily accommodate and reflect changes.
- Ensure that project is tied to clear business need.
- Evaluate multiple project alternatives, including a "do nothing" alternative.
- Ensure that requirements are clear and locked down prior to design, build, or purchase decision is made.

- Build sufficient time into the project schedule to perform application, integration, and performance testing.
- Require periodic project reviews; revisit justification, budget, scope, and schedule when assumptions change.
- Specify commercial off the shelf software which conform to industry standards and protocols whenever possible.

In addition to recommendations for managing technology costs within PSO organizations, recommendations which will lead to cost savings across the PSO industry are provided. These include:

- Industry stakeholders should continue to work together to "push" vendors to adopt more open architectures that are hardware- and database-independent.
- Industry stakeholders should continue to work together to adopt information technology standards to reduce costs across the industry. The development of common reference architecture and the adoption of the EPRI CIM standards are good starts.
- Industry stakeholders should continue to work together to encourage software vendors to develop more flexible solutions. Internally developed PSO solutions should follow the same principle. Adoption of more flexible architectures and design (like the recent Security Constrained Unit Commitment (SCUC) work completed by Areva, Siemens, and ABB) will lead to an increased ability to transfer technologies between organizations and promote a higher degree of interoperability.
- Governance, adherence to SDLC and Project Management methodologies, and strong vendor management practices will provide the discipline required to implement large PSO applications projects with fewer cost overruns and delays. Stakeholders must realize that implementation schedules and cost estimates must be based upon sound adherence to these principles and not emotional political appeals.

B. The Role of the Information Technology Organization

IT organizations exist to support the attainment of business objectives and goals. IT groups in Power System Operations organizations provide two primary technology functions: corporate governance and business unit support. In the corporate governance role IT is responsible for managing and protecting the technology investment of the organization. Policies, procedures, guidelines and standards are set to ensure that:

- Existing technologies are operated and maintained efficiently and effectively,
- New technology is developed and deployed on-time, within budget, and integrates easily into the existing environment, and
- The company's critical data, information, and systems are protected and secure.

In the business unit support role, IT is responsible for ensuring that each business unit's unique technology needs are fulfilled in the most cost effective and efficient manner. IT and the business units work jointly to identify the service levels and technology requirements that the business can afford; and establish operating procedures and project management processes to ensure that new and existing technologies meet availability, reliability, and cost criteria.

IT organization structures and reporting relationships vary widely across the industry depending upon the size, function, and business structure of the Power System Operator's organization. Nevertheless, the fundamental purpose of supporting applications and technologies, cost elements and project types are very similar. Consequently, common IT cost management best practices, based upon both industry-specific experience and standard technology management principles can be identified. The ability of an IT organization to effectively manage the cost to develop, deploy and maintain technology is dependent upon the:

- Degree to which the organization is aligned with the goals and objectives of the rest of the organization,
- Level of visibility into and control over on-going costs that the organization demands, and
- Rigor with which project management standards are followed and life cycle costs are managed.

Criteria for assessing the degree of IT and business alignment within an organization are presented in the next section, along with common cost categories and strategies for managing both on-going and project related technology costs. The prudent Business Manager, Regulator, or Director can utilize the adherence to the concepts presented in this section as indicators of the organization's ability to effectively manage technology costs. In addition to best practices for managing internal technology costs, the power system operator industry can also work together to minimize the cost and time to deploy new technology and increase the ability to interact and communicate across boundaries and borders. The last portion of this section addresses strategic ideas for managing technology costs across the industry.

C. PSO Internal IT Cost Management Strategies

The information presented throughout this section is based upon the use of a total cost of ownership (TCO) model as the fundamental building block for the management of the cost to develop, deploy and maintain information technology. The total cost of ownership approach is based upon the premise that all of the costs required to purchase, install, maintain and retire an

asset over its life time should be considered when evaluating alternatives and making purchase decisions.

1. Effective IT Organizations

Organizational effectiveness and bench marking studies indicate that IT organizations who invest the time and resources to develop rigorous business and cost management policies and procedures perform better than organizations that do not. The Total Cost of Ownership (TCO) is lowered, service levels are higher, projects are delivered on-time and within budget, and earnings tend to be more stable. These IT groups understand their purpose and role within the business and are provided with the level of corporate and business unit sponsorship that is required to effectively perform both their corporate governance and business support roles. Characteristics of these highly effective IT organizations include:

- Clear Purpose, Strategy and Business Alignment.
- Integrated, Routine, and Flexible Planning.
- Committed, Effective Leadership and Governance.
- Skilled, Experienced, and Productive Employees.
- Clear Roles, Responsibility, and Accountability.
- Well Defined, Documented, and Communicated Processes and Standards.
- Project Management Discipline.
- Operation and Service Orientation.
- Architectural Aligned Investment Strategy.
- Performance and Cost Measurement Management and Reporting.

When reviewing, auditing or assessing the effectiveness of IT organizations, prudent managers look for evidence of the performance as well as the existence of best practices. Simple reviews of process descriptions and operating guidelines are not sufficient. Project plans, status reports, cost reports, budgets, service level agreements, performance metrics, and operating logs must be reviewed to validate that planned and intended actions are being taken. Performance Indicators that can be used as evidence that the IT organization is being managed effectively and is developing technology which is aligned with the needs of the business organization include:

- A documented IT Plan linked and aligned with the Business Plan.
- Routine and consistent IT budget, cost and asset management reporting processes.
- Implementation and use of a rigorous Project Justification process.
- Implementation and use of a rigorous Project Management process.
- Implementation and use of a rigorous Vendor/Contract Management process with service level agreements (SLAs).
- Implementation and use of a rigorous Systems Development Life Cycle (SDLC) Methodology.

2. The Power System Operation Organization Technology Environment

The Information Technology environment which supports technology intensive businesses can be broken into three primary layers (1) the technical infrastructure, (2) corporate applications, and (3) business applications[5]. Power System Operations organizations follow this model well. Figure 13 below provides an overview of the three layers for typical Power System Operators.

a. Technical Infrastructure

The technical infrastructure is the basic building block of the technology environment. This includes the facilities, equipment, hardware and software required to support the centralized and distributed communications and computing needs of the organization. The servers, router, switches, lines, facilities, computers, operating systems, and software which comprise this layer can not be linked to a specific line of business or unique business function and are generally required to support any business regardless of the product or service provided.

b. Corporate or Enterprise Applications

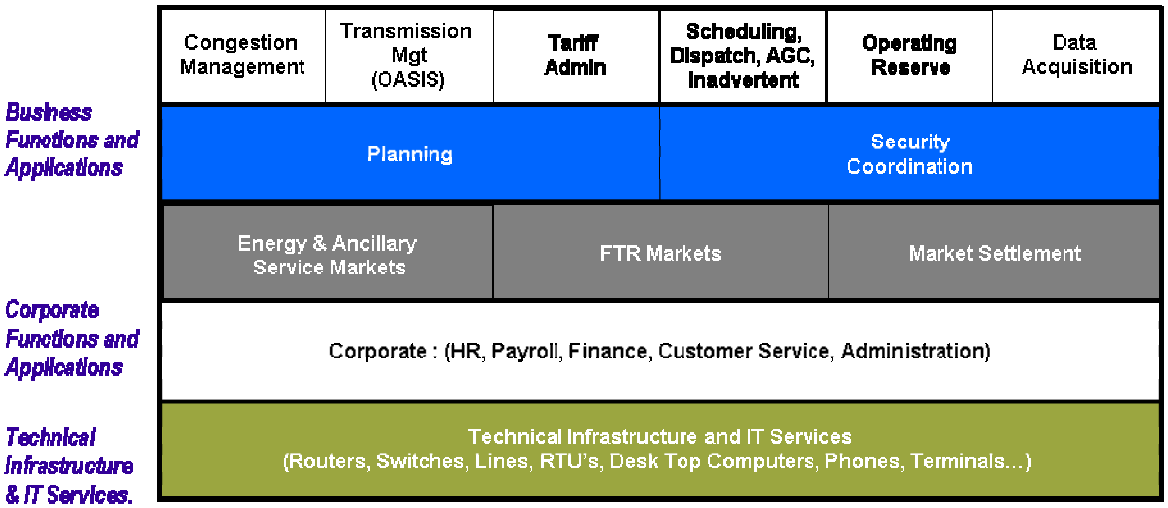
This layer also represents technology which is required to support the generic business functions regardless of the products and services which the business provides. This layer includes the system, hardware and software required to support corporate functions like HR, Finance, Supply Management, Legal, and even Information Technology.

c. Business Applications

Business applications represent the systems, hardware, and software required to carry out the specific and unique business functions of the organization. As illustrated in Figure 13, the top three slices represent the business applications layer of the PSO that exist to support the various Power System Operator functions. The top slice represents the applications that are required to provide basic Reliability Management and Control Area functions. The second slice represents the applications that are required to support regional planning and coordination function and the third slice contains those applications necessary to support Market Operations and Settlements.

[5] The business applications for PSO organizations can be further broken down in five distinct areas that are discussed in other portions of this document.

d. Figure 13 – PSO Technology Foundation and Component Elements



An understanding of the elements of the technology environment provides the manager, regulator, or director with the context to begin to understand the justification for proposed technology spending. All new technology projects and spending requests must be linked directly to one of these technology elements or to the implementation of a best practices process improvement initiative. The business function / applications matrix presented in Appendix J provides an indication of which business functions are supported by specific Power System Operator applications. Clearly, requests for spending on specific applications should be accompanied with a justification that indicates how the performance of the business function will be enhanced by the proposed expenditure.

As Power System Operator organizations evolve and begin to provide additional services, the investment in all three layers of technology also grows. The infrastructure and corporate applications layers tend to grow as the size of the organization expands. These investments are typically driven by the number of employees, sites, facilities, and customers of an organization. The business applications layer grows with the functions and services that organization provides. Reliability Coordinators which take on Control Area manager and Market Administration functions tend to require a significant investment in the business layer applications. This increase in both infrastructure and applications spending is illustrated in the graph presented in *Section II.A.* Figure 2. It is important to remember that Power System Operator functions are not typically independent of each other and the additional business applications to support new services or functionality typically require upgrades, enhancement, or interfaces to existing applications. These are costs which are often overlooked when project justification and initial funding requests are made.

3. Information Technology Costs

The costs to plan, build, deploy, maintain, and operate Information Technology can be divide into two macro-level categories for review and analysis when they are presented for approval (1) on-going operating costs and (2) project costs. Traditional utility financial analysts would argue that the appropriate categories are O&M and Capital; however, that distinction is made for determining financing requirements and rates, not for evaluating budget appropriateness and cost efficiency.

a. On-going Operating Costs

On-going operating costs represent the costs required to manage, operate, maintain, and routinely upgrade the applications, systems, hardware, and infrastructure that have been deployed and are being used to operate the business. This would include the entire annual information technology related coast regardless of the internal organizational budget in which they reside. (Many organizations unknowingly underestimate the size of their annual IT spend by including only costs that are under the direct control of the CIO. The cost of SCADA systems, plant and process monitoring equipment and distributed desk top computing are examples of costs which should be captured to understand the organization's total IT spend). On-going costs should be budgeted monthly, tracked and trended, compared to forecast, prior periods, and industry standards, and defended annually. Prudent cost management practices dictate that managers identify and track drivers for on-going operating costs. The table presented in Figure 14 provides a summary of the on-going technology costs and drivers for Power System Operations organizations.

b. Figure 14 – PSO Technology Foundation and Component Elements

Category	Cost Elements	Drivers
IT Management	▪ CIO & Staff Functions – budget, planning, HR, Supply …	▪ FTEs
Applications Support	▪ Staff, Licensing Fees, Maintenance Fees, Hardware Support & Lease Expenses, Consultants	▪ Number, size & complexity ▪ Number of servers and environments ▪ Release schedule ▪ Maintenance approach
Technical Infrastructure	▪ Router, Switches, RTU's, back-up sites, facilities costs, servers, storage, utilities, Line leases, etc…	▪ Number of sites, users ▪ Geographic footprint ▪ SLAs (back-up requirements, response times, availability)
Desktop Computing Services	▪ PCs, printers, software, licensing fees, servers, Desk side support/help desk, maintenance.	▪ FTEs
Communications Services	▪ Phones, Pagers, PDAs, Cell Phones, usage charges, maintenance	▪ FTEs

IT operating costs tend to grow as the organization grows. Expense categories like communications service and desktop computing services increase nearly linearly with the number of full time equivalent employees (FTE) that the organization supports since these

categories are largely comprised of personal computers, phones, pagers, printers, software licensees and other devices which support individual productivity and performance. IT management costs also tend to grow with the size and maturity of the organization, but should exhibit some leveling off and may actually decline on a per unit basis as economies of scale are realized. The drivers behind both applications support and technical infrastructure costs tend to be more specific in nature and require a more detailed review before judgments on justification of expense levels can be made.

Infrastructure cost can be driven by a number of different factors. For example, the number of sites and users that are supported tends to drive local area network (LAN) and wide area network (WAN) costs, while the internal service level agreements regarding back-ups, system availability and response time can be a significant driver of server and database costs. In a similar fashion, applications support costs are driven by more factors than user support requirements. The number of applications supported, the frequency of applications enhancements and maintenance upgrades, and service level agreements for back-up, data retention, and availability can be significant application support coast drivers.

c. Operating Cost Management Strategies

IT organizations can employ a number of strategies to manage and control on-going IT operating costs. At a minimum, operating expenses should be tracked and trended to evaluated reasonableness and identify potential problem areas. Cost drivers, linked to measurable business parameters, should be identified and tracked and trended as well to provide leading indicators of potential shifts in expense levels. This information should be routinely shared with operating groups and business leaders and they should take an active role in managing technology costs. Other strategies which tend to minimize the on-going costs of technology include:

- Employ organization-wide technology standards for architecture, hardware, software, operating systems, databases, and protocols to minimize development, maintenance, and support costs. Common and open architectures, protocols and platforms enable reuse, ensure interoperability and reduce costs.
- Maintain up-to-date policies, procedures, guidelines and configuration documentation to minimize maintenance and replacement costs.
- Employ release management, refresh, and retirement strategies to manage total life cycle costs.
- Employ supply and contract management strategies to maintain checks and balances with vendors.
- Track, trend, and analyze usage and cost data to identify cost management opportunities.
- Provide user organizations with usage and cost data to enable frontline cost management.
- Maintain an accurate asset database and link it to warranty, license, maintenance and support agreement information.

d. Project Based Costs

Project costs are the costs associated with deploying and implementing new applications, systems, hardware, and infrastructure to support the attainment of critical business goals.

Projects are typically driven by the need to provide new services, enhance performance, avoid significant risks, or repair/replace/upgrade existing technologies. Projects should have well defined objectives linked to specific business initiatives, clear justification including alternative analysis and total cost analysis, and detailed implementation schedules with start and end dates and periodic check points to assess the continuing viability of the project based upon performance and changing assumptions. Figure 15 below provides a summary of typical project related technology costs and drivers for PSO organizations.

e. Figure 15 – Project Based Cost Drivers

Categories	Cost Elements	Drivers
Initial Implementation Costs	▪ Direct Labor ▪ Hardware ▪ Software ▪ Systems Management ▪ Consultants	▪ Size, complexity and number of applications ▪ Duration of project ▪ Availability of off-the-shelf products, packages, and standard solutions. ▪ Degree of customization ▪ Competitive nature of market
Additional On-going Costs	▪ Support Costs ▪ Staff Related Costs ▪ Infrastructure Costs	▪ Number, size & complexity of applications ▪ Number of servers, storage devices, environments ▪ Release schedule ▪ Maintenance approach…. ▪ Number of sites, users, geographic footprint…

Much attention has been paid to the cost and time required by PSO organizations to design, build and deploy applications and systems to maintain reliability and manage markets. Projects seem to routinely come in over budget and behind schedule. Rework is common and the functionality does not always meet user requirements. The problems have plagued all type of applications projects from entire system replacements to accommodate changes in market structure to small enhancements of unit commitment programs. Surely the complexity of the PSO organizations and the level of internal and external interoperability that is required make the task of upgrading existing and implementing new applications difficult. The list of PSO applications provided in Figure 12 of *Section II.* includes 30 applications, many of which have multiple sub-components and multiple external interfaces. Nonetheless, similar complexity exists in the telecommunication, banking, and defense industries where processes and procedures have been designed to effectively manage technology.

Essential elements of a robust strategy to control applications development project costs are adoption and adherence to a common Project Management approach, a Systems Development Life Cycle (SDLC) methodology, a well communicated set of technology standards, and a total cost of ownership justification process. A SDLC methodology is a process for managing all of the required steps in the technology development process (from requirements gathering through design, build, test, deploy and maintain) to ensure that the deployed product actually meets the user requirements. Many SDLC models exist and all have their own merits. Experience has

proven that organizations which adopt and adhere to a standard SDLC model routinely deliver projects with fewer delays and cost overruns than organizations that do not.

SDLC processes help to ensure that the delivered product meets the business, technical, and functional requirements of the organization while adoption and adherence to a common Project Management process ensures that the project schedules, scopes and budgets can be effectively managed. Again, many project management processes exist and all have their own merits, but the essential elements of them all include the assignment of clear responsibility, accountability, and authority for completing the assigned tasks on time, the establishment of effective project controls and routine progress, status and risk reporting. Appendix A, *Section VI. J.* contains a detailed overview of project management and planning best practices.

The adoption and use of technology standards typically requires the evaluation and selection of a single technology or small set of high interchangeable technologies as standard solutions for common enterprise-wide requirements. Standards can be developed for any technology, but are typically most effective when economies of scale or the potential for multiple reuse exists. Technology standards for hardware (servers, PCs, phones, switches, and infrastructure elements), operating systems, communications protocols, architectures, and system development tools are commonly used to help control development, maintenance, and replace costs.

Cost analysis and project justification processes which are based upon total cost of ownership models help to ensure that rational economic decisions are made. In a total cost of ownership model the cost to design, build, manage, maintain, upgrade and eventually replace a specific technology are determined for each project alternative to ensure that an "apples to apples" cost comparison can be made. The initial costs to procure, build, and deploy the technology are combined with the expected on-going costs to maintain, support, and operate the technology and the future cost of replacement and retirement in a Present Value analysis to develop a total "life cycle" cost. While this is only one of the inputs to the project evaluation and justification process outlined in *Section V.*, it is essential to prudent cost management.

A quick list of additional strategies for maintaining control over technology project costs includes:

- Build flexibility into the design. Reliability policies and rules will change over time and applications must be able to easily accommodate and reflect changes.
- Ensure that project is tied to clear business need.
- Evaluate multiple project alternatives, including a "do nothing" alternative.
- Ensure that requirements are clear and locked down prior to design, build, or purchase decision is made.
- Build sufficient time into the project schedule to perform application, integration, and performance testing.
- Require periodic project reviews; revisit justification, budget, scope, and schedule when assumptions change.
- Specify commercial off the shelf software which conform to industry standards and protocols whenever possible.

4. Information Technology Budgets

Figure 16 below illustrates the form an organization's annual IT budget summary might take if it were presented for review and approval. While detailed review of IT spending and process adherence should be left to managers and auditors, the regulator, director, or senior executive should ask for more that single line item or single period budgets. On-going cost trends and forecasts should be tracked, reviewed and compared to the movement in the associated cost drivers. Similarly, project justification should reflect the total lifecycle costs and budget summaries should include spending to-date and total project spending, as well as current period costs. Additionally, changes in year-to-year project cost estimates and schedules should be tracked and analyzed along with changes in project assumptions.

a. Figure 16 – Sample Technology Budget

Annual Budget Summary

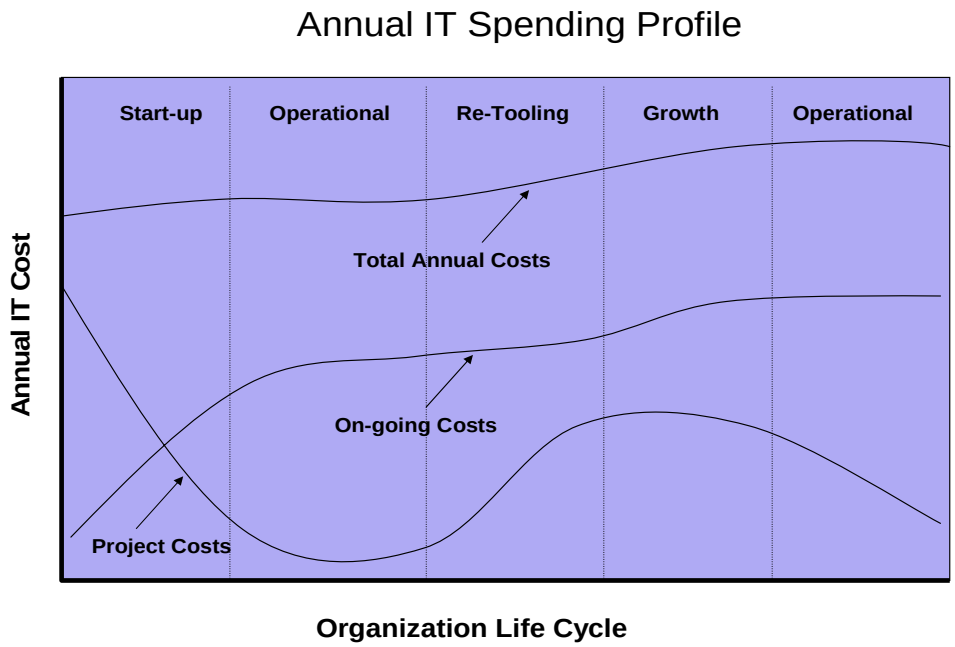
	$			Drivers		
On-going Cost	Prior Year	Current Year	Budget Year	Prior Year	Current Year	Budget Year
Management						
Applications Support						
Desk Top Services						
Comminications Servcies						
IT Infrastructure Costs						
Total	xxxx	xxxx	xxxx			

	$					
Project Related Costs	Prior Periods	Current Year	Budget Year	Future Periods	Total Project /Annual Forecast	Original Project Forecast
Project 1						
Initial/Implementation Costs						
On-going Cost						
Applications SupportCosts						
Additioanl Staff Related Costs						
Additionan Infrastructure Costs						
Project 2						
Initial/Implementation Costs						
On-going Cost						
Applications SupportCosts						
Additioanl Staff Related Costs						
Additionan Infrastructure Costs						
Project 3						
Initial/Implementation Costs						
On-going Cost						
Applications SupportCosts						
Additioanl Staff Related Costs						
Additionan Infrastructure Costs						
Total Project Costs						
Initail Implementation Costs						
Additional On-going Costs						

The relative percent of an organization's annual IT costs (which are comprised of on-going and project-based expenses) varies depending upon the maturity of the organization and the age of the supporting technologies. During start-up or the movement from one business model to a new business model (i.e. movement from a Control Area manager to a Reliability Coordinator or from a Reliability Coordinator to a Market Administrator) an organization's cost profile will be project-based with a much large proportion of annual spending being allocated for the development and deployment of new technologies. As the age and number of legacy

technologies deployed grows, the maintenance portion of the budget grows. In many cases as the age of a system gets beyond the normal useful life, maintenance costs can grow significantly and begin to outweigh the cost of upgrading or replacing the system.

b. Figure 17 – Annual IT Spending Profile



D. Industry-Wide IT Cost Management Strategies

The concepts and best practices presented above are required to effectively manage the cost to deploy and operate technology within specific PSO organizations. Gestalt was also asked to comment on strategies and approaches which industry stakeholders can employ and advocate to aid in the management of the costs to deploy and operate critical technology across the industry. The recommendations developed are listed below.

1. Industry stakeholders should continue to work together to "push" vendors to adopt more open architectures that are hardware- and database-independent. The use of hardware and database independent software:
   - Reduces the cost of operations by allowing common hardware platforms to be used within an organization.
   - Hardware can be reused.
   - Common skill sets are exploited.
   - Hardware maintenance cost is reduced.

- Reduces the cost of operations by allowing common database platforms to be used within an organization.
- Support is simplified (e.g. backup & recovery).
- Common skill sets are exploited.
- Software maintenance cost is reduced.
- Data access by external technology services is simplified.
- Reduces risk of technical obsolescence.
- Reduces the cost of software acquisition as one application can be purchased and integrated with other applications from another software vendor.

2. Industry stakeholders should continue to work together to adopt information technology standards to reduce costs across the industry. The development of a common reference architecture and the adoption of the EPRI CIM standards are good starts. Further development of Information Technology Standards:
   - Creates a common definition of key data elements.
   - Promotes efficient data exchange between internal and external systems.
   - Minimizes platforms required to exchange data with multiple entities.
   - Enables interoperability between multiple vendors' systems / tools.
   - Enables common user interface across applications.
   - Enables security considerations to be more uniformly approached and addressed.
3. Industry stakeholders should continue to work together to encourage software vendors to develop more flexible solutions. Internally developed PSO solutions should follow the same principle. Adoption of more flexible architectures and design (like the recent Security Constrained Unit Commitment (SCUC) work completed by Areva, Siemens, and ABB) will lead to an increased ability to transfer technologies between organizations and promote a higher degree of interoperability. Examples of flexibility enhancing design criteria include:
   - Business rules are separated from system code so Stakeholders can modify them without affecting the underlying code base.
   - Modular system design should be used when appropriate.
   - Non-proprietary coding languages are used.
   - Assessment of longer term migration to web services must be conducted considering any security constraints that may exist.
   - Security approaches and protocols are planned for and built into applications.
   - Off-the-shelf software should be used to facilitate system development where appropriate.
4. Governance, adherence to SDLC and Project Management methodologies, and strong vendor management practices will provide the discipline required to implement large PSO applications projects with fewer cost overruns and delays. Stakeholders must realize that implementation schedules and cost estimates must be based upon sound adherence to

these principles and not emotional political appeals. If the following pitfalls can be avoided, project costs and schedules will become more predictable.

- A lack of common market rules typically result in significant application modifications and increased costs for each new function and market.
- Continually changing market rules and ambiguous specifications and requirements typically result in costly redesign and coding.
- Bypassing the planning, analysis and design phases of applications and interface development projects and proceeding directly to vendor coding forces a tradeoff between costly rework and meeting stakeholder needs.
- Setting an unattainable schedules results in:
  - rushed planning and under-researched solutions.
  - less informed decision making, poor/costly technology selections.
  - over-reliance on vendors.
  - higher overall costs.
- Inadequate design/capacity planning driven by short implementation time frames will result in shortened system life and require large and costly replacements.

V. Performance Metrics

A. Section Summary:

In this section the metrics which should be developed, measured, tracked and reported on to assist management and IT operations personnel in determining the effectiveness of the deployed technology and the organization and pinpoint areas for improvement are described.

A PSO's overall organizational performance is heavily influenced by its IT organization's performance since the PSO's business functions are critically dependent on the applications and technical infrastructure as discussed in *Section II.* In order for the IT organization to perform at a very high level, it needs to institutionalize the process of measuring its performance. If its performance is not being measured, it is questionable if the IT processes and functions are being properly managed. In addition, performance measurement enables management to determine what areas are in need of improvement and what effect the improvement initiatives have had on performance. IT organizations that have not instituted a formal process should initiate the following activities to establish a performance measurement function:

a) Identify corporate and IT organizational goals.

b) Determine what IT processes and functions are linked to, and contribute to the attainment of, the corporate and IT goals.

c) Determine what performance metrics associated with the IT processes and functions identified in Step b accurately measure the IT organization's contribution to the corporate and IT goals.

d) Determine short and long term targets for each performance measure that will be used as the standard for performance.

e) Begin capturing and reporting the performance data in a manner that can be sustained without an inordinate investment of time.

f) Analyze the results of the performance measurement and determine the areas that need the most improvement.

g) Determine the improvement initiatives that are necessary to achieve the performance goals and quantify the time and cost that is necessary to achieve them.

h) Review the results with the internal and external stakeholders and gain their concurrence on prioritization.

i) Establish an owner for the performance measure and improvement initiative so that accountability is clear.

j) Continue measuring performance to gauge the effect of the improvement initiative.

k) Establish mechanism to benchmark performance against external organizations to search for additional best practices and opportunities for improvement.

Performance metrics should be captured in three critical areas: 1) System and Application Performance, 2) IT Service Delivery, and 3) Project Delivery. This section describes these three areas in additional detail.

B. System(s) and Application(s) Performance Metrics

System and Application Performance Metrics are designed to capture performance on specific systems (e.g. Server #1, Storage Area Network, PBX) or specific applications (e.g. Day-Ahead Security Constrained Unit Commitment, Financial application). The following list depicts examples of performance measures that should be captured:

- **System(s) and Application(s) Availability** – measures the time that the system is available for use by end users. The measure reflects the ability of the IT organization to keep the business productive with the system. Scheduled maintenance outages are generally removed, though, measuring the amount of total unavailability could be critical to ensure that maintenance outages are not excessive. This metric should also be captured for network components.
- **System(s) and Application(s) Performance** – measures the ability of the system to process information in an acceptably short period of time. End to end performance (i.e. from the time the user enters information until the time the result is displayed) should be captured to include network performance.
- **Job Success Rate** – measures the percentage of jobs that complete successfully and do not require intervention.
- **Defect Frequency for System(s) and Application(s)** – measures the number of functional and/or technical defects that have occurred with the system/application/component. This measures how stable the application is or whether it is frequently causing disruptions to the business or customer.
- **Time to Resolve Defects** – measures that elapsed duration that is required to analyze, fix, and implement defects that have occurred.

These previous metrics are indicators of how well the IT organization is performing. The ultimate IT metrics indicate how well the application is contributing to the organization's business processes and related goals. When an application is introduced, its usage should be focused on improving business processes and meeting organizational goals. Initially, improvements in the business process may not be seen; improvements generally occur over some period of time as users make use of the system to greater degrees. Therefore, it is advisable that organizations capture three types of information when an application is first introduced:

- **Usage of the application** - measures the extent to which the application is being utilized. Low usage in a particular area may point to training or usability issues. For example, the number of energy bids per week would measure how much the system is being used.
- **Business process metrics** – measures the degree to which the business process has been improved. This measure helps to quantify the extent to which the application is helping the business perform its work. For example, the number of times that the day-ahead energy market is cleared by the agreed upon time would indicate how well the applications are assisting in the process.
- **Business value measures** – measures the degree to which the organization goals are being achieved. These metrics help to justify the implementation of the new application. For example, measuring the decrease in the market clearing price for

power would help determine the efficacy of the energy market that the applications support.

C. IT Service Delivery Metrics

Service Delivery metrics are designed to capture performance on the various services that the IT organization provides to its internal and external customers. The following list depicts examples of performance measures that should be captured:

- **Abandoned Call Rate** – measures the number of calls that are made to the Help Desk / IT Service Delivery hotline that are not answered promptly enough resulting in the caller abandoning the call.
- **Incident Response Time** – measures the amount of time that is required to respond to an incident (e.g. problem, security intrusion).
- **Problem Resolution Time** – measures the amount of time that is required to resolve a problem to the customer's satisfaction.
- **First Time Fix Rate** – measures the percentage of time that the problem can be resolved on the first call.
- **File Restoration Time** – measures the amount of time that is required to restore a damaged or corrupted file(s).
- **Time to procure/install equipment** – measures the duration between when an end user requests the procurement of new equipment/software and when it is installed.
- **Time for processing Move, Add, Changes (MAC)** – measures the amount of time that is required for an end user to request a MAC and for it to be performed.
- **Security incidents** – measures the number of times that the organization has been subject to virus attacks, unauthorized intrusions, or other security violations.
- **Application Backlog** – measures the number of application changes that have been requested but have yet to be implemented.

As IT organizations mature, they should pursue formal Service Level Agreements with their internal and external customers. As part of the negotiation process, each of the Service Levels should have performance metrics defined which are reported against on a regular basis.

D. Project Delivery Metrics

Project Delivery metrics are designed to capture performance on the projects and the project portfolio as they are being conducted. The following list depicts examples of performance measures that should be captured:

- **Requirements Traceability** – measures whether the agreed upon scope of the project was delivered as expected.
- **Schedule Adherence** – measures the percentage of milestones completed in agreement with the schedule.
- **Budget Adherence** – measures the project's adherence to the established budget.

- **Earned Value / Expense Incurred ratio** – measures the project's accomplished work compared to the incurred expense. Complex projects tend to be difficult to track as the resource usage and expense incurred may differ from what was originally planned during the project baseline. A complex indicator that shows a ratio of the work accomplished compared to the cost incurred allows the Manager to understand if the project will complete on budget.

E. Organizational and Cost Metrics

Organizational metrics are designed to capture performance of the organization as a whole. Cost metrics identify the expense that is being incurred in the provision of services. The following list depicts examples of performance measures that should be captured:

- **Customer Satisfaction** – measures the degree to which the internal and / or external customers feel that their expectations are being met. This data is usually captured through a formal survey technique.
- **Support Personnel per customer** – measures the number of IT personnel normalized by the number of customers. This approach to normalizing the metric is used during benchmarking to allow for entities of differing sizes. It can be calculated on a service-specific basis, showing the number of staff providing a service relative to the number of service users.

F. Recommendations and Cautions

Creating and reporting on performance measures is subject to deliberate and accidental misuse. Improper reporting can lead to incorrect conclusions. The following are suggestions to ensure that performance reporting achieves its goal of accurately conveying the current state of performance:

- Performance charts should show the actual data compared against the goal. It should clearly state what the chart is measuring and why it is important
- Caution should be exercised in showing rolling averages of performance metrics. Outliers will significantly affect the rolling average and distort the conclusion. If an outlier that reflects poor performance recently occurred, performance will look worse; as the outlier moves out historically performance will be artificially inflated. Trend line (excluding outliers) if they are statistically significant should be used to reflect performance trends.
- Changes in the environment or service should be annotated on the chart so that the effect can be easily seen.
- Performance metrics that use averages should be used with caution. The distribution of scores is often important in understanding total performance. For example, the average time to resolve problems may be very low. However, if there are a small number of critical problems that take a very long amount of time to resolve, simply showing the average may be misleading. Showing the distribution of times required to resolve problems is an excellent way to deal with this limitation.
- The use of macro indicators (e.g. IT cost per MW) can be misleading as the cost to operate an IT organization is not linearly dependent on the size of the entity. Some

economies of scale should be realized as the entity grows larger. In addition, using revenue in the denominator may distort the conclusion if the organization's revenue is driven by regulatory mandate.

- Performance indicators that use headcount measures may lead to incorrect assumptions. For example, a performance indicator that tracks the number of support personnel per customer may not be comparable from one organization to another since one organization may use contracted services to perform the work. Cost is generally a safer approach than head count.
- Performance indicators that show the percentage of cost for different categories may be misleading. For example, the percent of an organization's cost that is dedicated to internal employees may be artificially lowered if the total cost for that organization is higher than other similar entities.
- Performance indicators that are cost-oriented may be unfairly affected by lease vs. buy decisions. Organizations that lease equipment will show higher costs year-to-year while companies that buy equipment may not reflect the acquisition costs in the year that they were incurred.
- Average salary analysis need to be interpreted in light of the geographic area in which the organization resides as well as the staffing strategy that the organization has pursued. For example, if an organization outsources lower level work, its average salary per employee will be higher than other organizations.
- Performance indicators that depict processor utilization metrics are difficult to interpret. Low processor utilization may be a result of an organization that has tuned their systems to run efficiently. On the other hand, low processor utilization may also reflect a strategy of buying more capacity than is required. Processor utilization is more appropriately used for capacity planning than performance measurement.

VI. Power System Operation Critical Technology Issues

A. Section Summary:

In this section the specific questions that the FERC staff asked Gestalt to address as part of this study are answered. Where applicable the answers include a discussion of the issues which must be considered and a review of recommended analysis approaches.

The specific questions addressed in this section are:

- How should the Buy vs. Build decision be approached?
- What PSO technologies should be considered for recycle and reuse?
- When should applications and projects be abandoned and "sunk costs" ignored?
- What should be considered the normal life span of PSO technologies?
- What are the issues that arise when a limited number of vendors participate in a technology market, and how can the risks be mitigated?
- How should cyber security concerns be addressed in the IT acquisition and development process?
- What is the impact of excessive delays when new technology is being implemented?

B. How should an entity conduct the Buy vs. Build evaluation/decision-making process?

1. Definition: Buy vs. Build

When a Power Systems Operator[6] (PSO) is looking for an application software solution to satisfy a business need, it is faced with making an implementation decision from among the "Buy vs. Build" continuum of customization approaches. The PSO can also look at alternative approaches such as leasing and outsourcing, though this approach has been seldom used for energy related applications. This discussion is limited to four general categories along the "Buy vs. Build" continuum. The four categories are:

Buy: Purchase an "off-the-shelf" commercially available solution and install with little or no changes. Generally these solutions are mature commodities/utilities that are standard within and/or outside the industry (i.e. email, collaboration tools, desktop word processing and spreadsheet applications, system/network management).

Buy and Configure: Purchase a commercially available solution and configure a limited amount of features, data fields, work flow, and reports to meet the unique requirements of the business (minimal application development). These solutions are usually related to generic business functions (AP/AR, G/L, Purchasing, HR, etc) that are standard within and/or outside the industry. This category also includes some PSO industry specific transaction processing/engineering applications that have existed for a long time with little changes to the business processes/data where there is little differentiation within the industry. These systems generally include Energy Management Systems (EMS) and associated power system analysis applications that are required for reliable system operation. With regard to systems and applications related to market administration and operation, some commercially available solutions may be applicable as long as the PSO is willing to adopt the market business rules associated with that solution. For example, ISO New England obtained day-ahead market clearing and real-time market clearing and dispatch software that was developed for the PJM Interconnection with lesser configuration required because ISO New England adopted the related PJM business rules.[7]

Buy and Customize: Purchase a commercially available solution and significantly customize the functions, database, user interface and process flows to meet the unique requirements of the business (significant application development). These solutions are usually transactional, market operations, and limited information management solutions that contain a baseline set of common functions/data, but generally don't meet the needs of the specific business rules/processes and unique data requirements and reporting of the PSO without the customizations. For example, with regard to market operations applications, not all real-time markets are designed to clear on a Locational basis (i.e. LMP based). However, the reliability based real-time dispatch software will contain the algorithm to perform security constrained economic dispatch. The real-time dispatch software will need to be

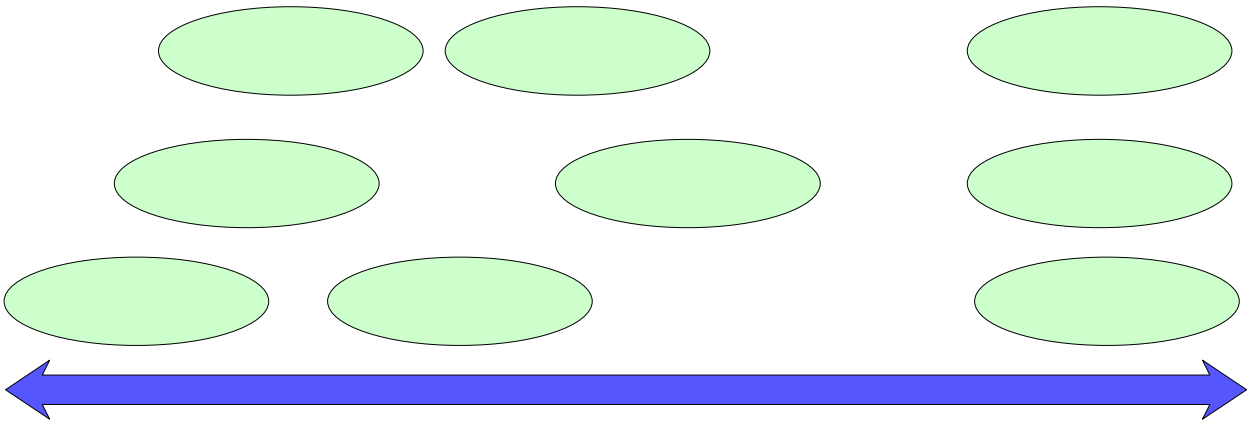
[6] A PSO could include a Control Area operator, a Reliability Coordinator, an ISO or an RTO.

[7] ISO New England implemented their Standard Market Design (SMD) that was based on PJM's market design on March 1, 2003. PJM had contractual rights to resell the commercial software that was part of the overall solution.

customized to calculate real-time clearing prices in accordance with the particular market design. Real-time dispatch applications that calculate Locational Marginal Prices are the most readily available.[8] Over the last five years, market standards have emerged which have become the foundation for several software product offerings. These products should be able to serve as the basis for any new market solution where the market is based upon the FERC Standard Market Design. The adoption of these products should reduce the amount of customization that is required to implement the solution and reduce the number of situations that justify building new software applications from scratch.

Build: Develop the solution "from scratch" based upon the detailed design created to meet the business requirements. This involves extensive application design, development and testing, and may be done with either internal or external (consultants) resources. These solutions involve a highly specialized business function for which no viable commercial software exists (or commercial software is built upon aging technology and won't support future needs) or the solution is for a business function that could be a market differentiator vs. competitors. Data Warehouse/Data Analytics/Business Intelligence and Customer Portal applications tend to fall in this category. Market settlement systems are a prime example of systems that must generally be built from scratch due to a lack of commercially available applications.

a. Figure 18 – Buy vs. Build Continuum



Most Power Systems Operator's transaction and information management software solutions will fall in the "Buy and Configure", "Buy and Customize" or Build categories. For ease of discussion, when "Buy" is identified in the following text, there is a presumption that it is "Buy and Configure" or "Buy and Customize".

2. Decision Making Factors

There are many factors that should be considered in determining the best implementation approach for the given business need. Within their defined role as Control Area Operator, Reliability Coordinator, or Market Operator, most Power Systems Operators will perform the same functions and capture, analyze and make decisions based upon the same general set of

[8] Both Areva (formerly ESCA) and ABB offer LMP based day-ahead and real-time market applications.

data (i.e. SCADA). However, each PSO will have its own unique organization vision, strategy, core competencies (IT and business), marketplace (stakeholders), regulatory/reporting requirements, geography, and other factors to consider when evaluating its software application needs. To make the decision regarding the different approaches, the Power System Operator should consider the following:

- **Business need flexibility** – adopt a standard market design that is in line with available market applications.
- Uniqueness of need/business value – commodity vs. differentiator
- **Availability of viable commercial solutions** – proven installed base, meets 80% of functional requirements
- **Technology fit** – solution alignment with current/planned technical architecture
- **Time to market** – need to implement solution by a given date
- **Total cost of ownership/ROI** – overall cost of solution from concept to retirement and return on investment
- **Risk** – scope creep, schedule/cost overrun, vendor dependence, etc. (see *Section V.A.4.* Buy vs. Build Decision: Risk Analysis)
- **Skilled and available resources** within and external to organization, technical, management
- **Vendor confidence** – experience, solvency, track record, product volatility
- **Expected/required solution life span** – temporary solution, long term keystone component in overall architecture
- I**T architecture portfolio and strategy** – standard architectural components, mix of built vs. bought applications
- **Corporate strategy regarding role of the internal IT department** – strategy/architecture, systems integrator, in-house development, maintenance in/out-sourcing, etc.

These factors and others will be referenced in the following sections that describe the general processes that should be followed when making the buy vs. build decision.

3. Methodology

No decision regarding the choice of buying a commercial "off-the-shelf" solution or building a custom-made application should be made until the business needs are well articulated and documented, and planning and analysis is completed. Many organizations tend to harbor a predefined bias regarding either always selecting and installing commercial solutions, or always custom building all applications that support transaction processes. Neither approach is wholly right or wrong. We recommend that each business need that requires a software solution follow a formal evaluation process that considers commercial solutions where the decision is based upon objective criteria or factors such as those listed above.

Once a business need is identified that requires a software solution (e.g. Internal Market Monitoring function or Security Constrained Economic Dispatch), the PSO should follow its

Systems Development Life Cycle (SDLC) methodology to complete a Requirements Definition *(see Appendix A: IT Best Practices Guidelines – SDLC Methodology)*.

Generally, there are two to three opportunities to evaluate the feasibility of package selection during the early phases of a project and each is conducted during the Planning, Analysis, and Design phases (less often during the Design Phase). Each evaluation will serve a slightly different purpose, and will be aided by more process, data, and technical information with greater specificity. The following sections detail the approach for the Planning and Analysis phases. When the evaluation of package solutions occurs in the Design phase, it takes a similar approach as the Analysis phase but should be based upon a Conceptual Design Document (sometimes Physical Design as well) that is quite detailed. If the evaluation process is delayed until then, it is usually because an organization had previously decided to build the solution and is redirecting its efforts to consider buying. This may result from a change in original business needs such as timeframe, available resources; or new viable solutions that previously didn't exist or were originally deemed too risky.

a. Planning Phase – Commercial Package/Solution Availability

The initial evaluation of a Buy vs. Build decision starts in the Planning Phase, with the purpose of determining whether there are any viable commercial solutions in the marketplace that will meet the business need. The outcome will not produce a finalized buy vs. build decision, but will eliminate a "Buy" decision early on if it is found that there are no available commercial solutions in the marketplace. Generally within the PSO industry, there are very few functions that do not have commercially available solutions. Business Intelligence functions that involve Data Warehousing and Analytics and market settlement systems are a noted exception.

During the initial Planning Phase of a project, business requirements are not well known and often are known only at a high-level. However, the preliminary Requirements Definition that contains the baseline business functions and processes, high-level information requirements, and technical criteria (hardware, operating system, security, middleware, database, etc.) should be started in this phase. Once created, the following steps should be taken:

1. Define a list of criteria for the evaluation that includes key functions and features, technical requirements, vendor/commercial package facts, terms and conditions, implementation methodology and timeframe, and costs with breakdown into multiple categories.
2. Survey available commercial packages/solutions and vendors to compile a list of potential packages.
3. Prescreen vendors/solutions based upon "must-have" criteria from the evaluation list; request information from remaining vendors (2-5) based upon evaluation list.
4. Respond to vendor questions as needed, follow-up to obtain complete information from the vendors. *Arrange and view informal package/solution demonstrations.
5. Analyze collected information from the vendors, and compile a Package/Solutions Comparison Matrix by criteria to identify any viable vendor solutions.
6. Eliminate "Buy" option if no viable solutions are found or the technical architecture is incompatible. *optional – not necessary but can be helpful in providing ideas during the Analysis Phase.

Many organizations prematurely select a package/solution at this stage and skip right to package installation and modifications. They believe that they will save time and money by eliminating the Analysis and Design phases because it is not necessary to further define requirements or create a conceptual design. This is a critical mistake in the evaluation/implementation process and leads to significant schedule and cost overruns at best, and failed implementations at worst because it is discovered too late that the package cannot meet the business needs. Even if the package/solution is likely known at this point, it is imperative that the Requirements Definition is completed.

b. Analysis Phase – Buy vs. Build Determination

The Requirements Definition that was started in the Planning Phase will be completed during the Analysis Phase. Business processes will be defined at a more discreet level with data inputs and outputs included. Business rules will be agreed upon and documented. The conceptual database design, external and internal system interface requirements, and report requirements will be documented. Anticipated transaction volumes, service level requirements, and data redundancy and retention needs will be defined. The number of end users by function and location will be known. The technical architecture will be conceptually defined with specific component parts identified such as type, version and number of servers, operating system, database, security, user interface, remote and/or mobile access needs, middleware, etc.

With the completed Requirements Definition that details the business needs and the desired technical environment, the Buy vs. Build analysis can be completed. Assuming that there are still viable commercial Package/Solutions available, the following steps should be taken:

1. Identify Buy vs. Build analysis factors and establish a weighting system (see above *section 2*. Decision Making Factors).
2. Update the Package/Solutions Comparison Matrix with more specific functional and technical criteria derived from the Requirements Definition. Where appropriate, include the Buy vs. Build Factors relevant to package/solutions in the matrix (vendor confidence, etc.).
3. Perform formal package/solutions selection analysis that includes: Requests for Proposal/Solutions, Proposal/Solution evaluation, script cases, formal functional and technical demonstration reviews and scoring, vendor reference checks and reference site visits. Objectively determine the best choice package/solution.
4. In parallel with the selection analysis, determine the approach, timeline, resources, risks, and total costs for the Build alternative.
5. For the package/solution finalist, identify all known risks, determine customization requirements and technical infrastructure changes needed, confirm approach and resource needs, and adjust schedule and costs for the Buy solution accordingly.
6. Update the Package/Solutions Comparison Matrix to include the Build alternative and score and weight the Buy vs. Build analysis factors.
7. Select the implementation approach.

c. Buy vs. Build Decision: Risk Analysis

There is often a presumption that buying a package/solution is less risky than building one from scratch. The following are some questionable assumptions that support this idea, yet are often untrue:

- Buying a package/solution is significantly cheaper and has a more predictable total cost of ownership than a build solution.
- The vendor or third party integrator has experience implementing the software, so the time to market will be shorter and more predictable.
- The package/solution works because it has been purchased and installed elsewhere.
- The vendor is accountable for implementing the total solution.
- The software will better adapt to changes in the industry or technology because the vendor supplies the software releases or upgrades.

Each implementation approach has its own inherent risks associated with it. As part of the Decision Making Factors identified above, evaluation of risk is a critical component in determining whether to buy or build. It is important to compare the risks for each evaluated approach. Below is an example of the general risks to consider that may or may not be relevant to all situations. More specific risks should be identified for each approach.

d. Figure 19 – Buy vs. Build Risk Analysis

Risk	Buy (and/or configure/modify)	Build
Functional Risks		
	Vendor doesn't understand or misinterprets requirements and/or Evaluation team misinterprets vendor responses (fit is less than presumed)	Functional requirements are not well defined, or are not finalized before development begins
	Vendor/Third party integrator doesn't address legacy system and external interfaces	Functional requirements are based only upon a single organization's knowledge, not best practices within/across the industry
	Vendor doesn't assist with data conversion	The scope "creeps" and begins to include items that are not critical to the business.
	Business users aren't available to identify and design modifications	Business users aren't available to define requirements
	Business users won't accept system because it doesn't conform to their needs	Business users won't accept system because it doesn't conform to their needs
	Package may be difficult/costly to maintain and adapt to business changes	Functional requirements are "old" and outdated by the time solution is operational
	"Volatility" of product is high – frequent new/major releases or upgrades	
Technical Risks		
	The technology used is too old or too new (i.e. not mature)	The technology used is too old or too new (i.e. not mature)
	The software is/is not built with open source technology	The solution is poorly designed and architected impacting scalability, performance and usability
	Technical performance is difficult to predict/Production performance fails to meet targets	Technical performance is difficult to predict/Production performance fails to meet targets

Risk	Buy (and/or configure/modify)	Build
	Technical problems may be difficult and costly to identify and fix	Systems development, testing, and project management methodologies are non-existent or deficient
	Vendor may not provide enough technical support for your specific technical infrastructure	Technical staff lacks skills, knowledge, training and experience in technologies
	Interfaces may be more difficult to build based on package technology	Learning curve for technology used to build solution is high impacting schedule
	Internal Operations support may be unprepared to support new/foreign technology	Internal Operations support may be unprepared to support new/foreign technology
	Solution unable to adequately operate in customer technical environment	Technical stability of solution lacking, unable to implement
Other		
	Total cost of ownership (TCO) is undervalued due to inaccurate maintenance and upgrade cost projections (if less than 65-75% of TCO, probably undervalued)	Total cost of ownership (TCO) is undervalued due to unrealistic/unbudgeted labor costs
	Vendor's strategic direction unknown, difficult to influence, or focused on other customer needs	TCO is undervalued due to unbudgeted design, development, testing, configuration management, and deployment tools necessary to support project
	Vendor's financial stability difficult to predict, and merger and acquisition activity high in the specific industry	TCO is undervalued due to unplanned and unbudgeted need for multiple technical environments (development, integration, testing, QA, etc.) necessary to support project
	Vendor or third party resources may not be available when needed	Technical resources may not be available when needed to support design, development, testing, deployment and operations of solution
	Vendor development quality control and testing may not meet in-house standards	Development quality control and testing insufficient
	Unclear roles between vendor, third party integrators, and in-house staff can cause confusion, delays, and cost overruns.	
	Training and documentation is inadequate	Training and documentation is inadequate
	Less control over configuration/customization process, schedule, and quality, and insufficient Vendor management methodology	Inexperienced project/program managers unable to control scope, schedule and costs
	Contracts with vendors/third party integrators do not adequately define expectations and problem remedies	

If the ultimate solution involves a significant investment (i.e. >$5-10,000,000) and the potential risks could impact the financial benefits of the evaluated options, it may be necessary to use formal statistical risk analysis techniques. These techniques identify the potential cost of the risk, and the likelihood of the risk occurring as a way to measure the overall risk of each alternative. Risk mitigation strategies should be identified, and any additional project costs should be determined and added to the particular implementation approach alternative (example: configuration management tools, performance management tools/environments, third party project audits, etc.).

C. When a PSO organization is starting up, implementing new services, or revamping an existing service should they consider reusing the applications developed for other PSO Organizations?

The reuse of specific software products, custom code and application modules within any IT organization is one way to cut development costs and reduce the cycle time required to develop new applications. Open architectures, standard data definitions, and web services technologies are making this easier and internal reuse should continue to be an objective of well-run IT organizations. The reuse of applications developed for one PSO by another, however, has been much more limited and, for various commercial and operational reasons, is considered, at best, a questionable long-term strategy. As operations, market and business rules become more standardized, this strategy may become slightly more viable.

For purposes of this discussion we have defined two types of reuse: "complete applications reuse" and "partial product reuse". Complete applications reuse is the direct transfer and reconfiguration of an application that was developed by, or for, one PSO to another. In this case the initial PSO owns the code and is responsible for maintenance and support. Partial product reuse occurs when the buying PSO contracts with a vendor to purchase the same version of a product that the vendor developed for the initial PSO. The buying PSO then purchases the business rules, user and project documentation, system, interfaces, training manuals, and operating guides that the other PSO developed and uses them as a baseline to "kick-start" the development of their own support materials. The merits of both types of reuse are discussed below.

In this analysis, the reuse scenario where one PSO buys the proprietary code of an application that was originally purchased from a product vendor is not considered commercially feasible. When a software application is bought directly from a vendor and reconfigured, the buyer does not obtain ownership rights to the source code and is not allowed to resell the product. In actuality, the buying PSO would go directly to the vendor to buy the code and would consider a partial product reuse from the other PSO.

1. Complete Applications Reuse

The reuse decision is another form of the Buy vs. Build decision discussed in *Section V.A.* above. In this case the other PSO organization is essentially considered an alternate vendor and the reuse of its solution should be considered as another alternative in the analysis of the various buy options. In situations where one PSO owns the application code and is responsible for their own maintenance, upgrades, and enhancements, significant commercial and operational risk is introduced into the buy analysis.

PSO organizations are not software vendors and, in most cases, are not providers of commercial services. They are not resellers of technology and do not have the ability to provide warranty protection or the technical staff to customize, configure, maintain, or upgrade the application for the buyer. Generally, custom-developed software is not designed and developed in a manner that is conducive to migrating the software to another environment. Rather, the components have to be packaged and reassembled by the buyer. The buyer, therefore, must obtain the internal resources to install, maintain, upgrade, and enhance the application and has no real recourse if the application does not work properly or

cannot be configured to meet the functional needs of their organization. This risk may be mitigated slightly in situations where there is a perfect match in business, functional and technical requirements, but those cases are few and far between.

In most cases, the business, functional, and technical requirements are so vastly different that the cost required to reconfigure a customer built application for another PSO business approaches the cost to build an entirely new application. Consequently, only in extreme circumstances where a complete and thorough Buy vs. Build analysis has been done and it has been concluded that the complete applications reuse option is less costly and that the additional risks could be mitigated would this option be recommended.

2. Partial Product Reuse

Partial product reuse is also another alternative in the buy vs. build analysis. In this case, the actual product vendor supplies the code and configures the application to meet the business requirements of the buyer. It is expected that the total cost analysis should yield a lower overall project cost than a complete new buy for a similar product for several reasons. The initial cost of the configured software may be obtainable at a discount since the vendor will have already delivered the product version to the original PSO. In addition, the project-related support cost should be significantly lower since the business rules, customer interface, system interfaces, user documentation, project documentation, and training materials are purchased from the original PSO. More importantly, the time to implement the application should be significantly lower since the product and base line support materials have already be developed.

Several PSO organizations have adopted partial product reuse strategies for new market implementations, though, it is difficult to determine the extent of any realized cost or schedule savings. ISO New England purchased the support material for the PJM Day-Ahead and Real-Time market system[9], MISO based a significant portion of their market design on the PJM model, and both CAL ISO and ERCOT are exploring the use of eastern US market designs. All of these seem to be movements in the right direction and should yield positive results.

3. Common Architectures and Standards

While the initial attempts to reuse business rules and applications project support materials may produce positive results, truly significant improvements will only be obtained when products that incorporate open and service based architectures and common data standards are available. Integration and migration costs are some of the most significant costs associated with replacement of large scale systems. The ability to integrate applications introduced by these advancements should make reuse much easier and more common.

The efforts to develop and implement the Common Information Model (CIM) data standards and CME (Common Market Extension), the efforts of the ISO/RTO Information Technology

[9] Areva (formerly ESCA) and PJM formed PJM Technologies, a wholly owned subsidiary of the PJM Interconnection, LLC that markets the PJM Business Rules and associated market applications.

Council to develop a common reference architecture, and the efforts of the three primary providers of EMS products to develop common data definitions for Security Constrained Unit Commitment (SCUC) programs are all examples of positive industry progress and should continue to be embraced and endorsed by industry stakeholders.

As PSO IT organizations develop their own applications, they should look to create a services-based approach where applications are componentized and can be more easily reused by other applications. These services can then be invoked by third party software as the independent software vendors open up their architectures. In addition, the work that is being done to develop Joint Operating Agreements where multiple PSOs exchange and utilize data from other PSOs should be built upon a common services based approach as appears to be under way now by PJM, MISO and TVA.

D. When should an entity stop sinking additional investment into an existing application or the on-going development of a new application that has not produced the desired results and restart or reevaluate the alternative solutions, including the potential to implement another Power Systems Operator's solution that is already in place?

The above question should be broken into two separate discussion threads (1) Re-evaluation of an existing, under-performing application, and (2) Remediation of a troubled application development project. In thread one, we will discuss the process of assessing technology that has been in an operational environment, but is suspected or acknowledged to be underperforming. In the second thread, we will discuss actions to identify and respond to a failing application development project, as well as preventive measures to mitigate the risk of failure.

1. Re-evaluation of an existing, under-performing application

When an existing application that has been in an operational environment is suspected or known to perform below expectations, an assessment should be undertaken to determine the root cause of the underperformance. The assessment should produce an objective evaluation of the application regarding its future viability. Concurrent with the assessment, benchmarking within the PSO industry (external if warranted) of similar "best practice" applications should be conducted. At the completion of the assessment and benchmarking, alternatives (maintain, buy, build, etc.) should be compared and a recommendation for action made. The assessment is usually sponsored by the CIO or CTO within the organization. However, it is recommended that sponsorship reside with either the COO or CFO, because the ultimate decision is usually based upon a cost/benefit financial analysis, not just a technical analysis.

a. Application Assessment

The assessment is best conducted by an external third party who has experience with the application type in question, but who does not have a vested interest in the outcome of the analysis. The PSO technical and operational management should be involved in the assessment to provide relevant information about the application, technical environment, relevant supporting data center operations, business functionality, maintenance costs, planned process or business rule changes, and corporate strategy. The third party should have access to best practice information within the PSO industry, as well as outside where appropriate for the application in question. The assessment should evaluate at a minimum, the following categories:

1) Business Functionality

- Does the application adequately support each and every one of the current and/or redesigned business functions and processes of the user environment?
- Where it doesn't support the processes adequately, can the application be modified easily?
- Can the application support future changes to the business functions and processes due to regulatory mandates, business rule changes, mergers or acquisitions of other companies, etc.?
- Do the users have all of the information (data) within the system to execute their functions, generate reports, and perform analysis? Does the information flow seamlessly to other applications that use it (integration/redundancy)?

- Does the application provide adequate presentation, and visualization of information required to make time-sensitive decisions?
- Are business alerts or alarms built in and effective? Are the necessary decision support and business intelligence functions in place, accurate, timely and actionable?
- Are the appropriate and current training simulators in place to support the use of the application? Are operators/users/stakeholders trained in the functionality of the application?

2) Technical

- How old is the application, and is it technically stable (does it fail)? Is it secure?
- Are the technical components (database, middleware, language, security, etc.) current and industry standard? Are they consistent with the other applications being used? Can they be upgraded or replaced?
- Can the application adequately scale to accept increased volumes of data? Will it be able to still maintain regulatory performance standards?
- Does the application require specific hardware, software and communications equipment to operate? Are these included in future architectural standards?
- Are there many interfaces to other applications, and are they complicated? critical? hard-coded? Is the application a core component to the overall application architecture?
- Are there technical resources available and affordable to operate and perform modifications to the application when necessary?

3) Performance

- Does the application meet current regulatory (e.g. FERC) or industry (e.g. NERC) performance requirements? Will it be likely to meet future requirements?
- Does the application meet the performance service level agreements (SLAs) agreed to with the users – could be internal or external users (window response time, run-time, analytical calculation speed, query speed, etc.?
- Does the application meet the up-time (SLA)? If not, what are the root causes?

4) Cost

- What are the costs to operate the application? What are the costs to maintain the application and keep it current with business needs? What are the costs of system outages/downtime?

(See above section III. IT Cost Management Best Practices for detailed review of cost analysis)

5) Organizational Strategy

- Given where the organization wants to be in the future, will the application meet its needs?

- Will other PSOs take responsibility for the functions that the application is currently supported? If so, which particular functions, when, and what interfaces are required?
- Is the organization contemplating Business Process Outsourcing for the functions that the application supports?
- Are there any known/predicted external events within/outside of the industry that could impact the decision about this application? (e.g. compliance to Common Information Model)

To aid in the objective review of the application, an Application Assessment Scorecard should be created. The scorecard should list the above mentioned categories with details for each. Specific criteria to evaluate each category should be defined, as well as the relative criticality. This scorecard should be created before the data gathering and analysis begins, and agreed to by the Executive Management of the organization. Figure 21 provides the definitions for, and an example of, an Application Assessment.

b. Figure 20 – Application Assessment Scorecard: Explanation of Columns

Category	Criteria	Score	Criticality	Weighted Score	Notes
List the major categories and elements within each category.	**Identify the specific evaluation criteria related to each category/element, and assign a consistent point scale.**	**Identify the score for the category /element.**	**Define the importance of the category to create a weighting system. For example: 3 = Must meet highest criteria due to regulatory mandate, reliability/safety, or business operation 2 = Critical to the efficient operation of the business 1 = Important but not critical to efficient operation of the business**	**Score multiplied by Criticality.**	**Identify key findings related to the category and scoring.**

Category	Criteria	Score	Criticality	Weighted Score	Notes
Functionality					
Total Business functions and processes are supported	3 = >95% of required functions/processes supported 2 = >80% of required functions/processes supported 1 = >80% of required functions/processes supported, but don't meet user expectations 0 = <80% of required functions/processes supported				
Business Function/Process X supported **(note: list each function and/or process individually to evaluate)**	3 = function/process X is fully supported 2 = function/process X is supported, but user desires minor modifications 1 = function/process X is partially supported, but requires major modifications 0 = function/process X is not supported				
Information Requirements support	**(note: list the high level data, reporting and analysis requirements of the business)**				
Integration Requirements	**(note: list the application integration requirements from a business process/information point of view)**				
Technical					
Architecture stability	3 = No or rare technical component failures 2 = Rare component failures – no business impact 1 = Frequency of component failures impact business 0 = Frequency of component failures impact reliability and safety				
The application uses Database Brand X/Version #.#	3 = current and industry standard 2 = current but not industry standard 1 = aging 0 = obsolete **(note: list each technical component that is necessary to evaluate, given the future architectural strategy – security, middleware, server, communications, etc.)**				
Performance					
The application response time	3 = always meets or exceeds SLA 2 = meets or exceeds SLA 90% 1 = meets SLA < 75% 0 = rarely/never meets SLA **(note: plug in real SLAs)**				
Application availability	3 = Uptime >99.99% 2 = Uptime <99.99>98% 1 = Uptime <98>95% 0 = Uptime <95% **(note: plug in real SLAs)**				
Cost					
Maintenance Costs	3 = Each Modify Unit < $1,000 2 = Each Modify Unit < $5,000 > $,1000 1 = Each Modify Unit < $10,000 > $5,000 0 = Each Modify Unit > $10,000 **(note: plug in real $/FTE levels)**				
Operations Costs (labor)	3 = Monthly Ops Cost < $5,000 2 = Monthly Ops Cost < $10,000 > $5,000 1 = Monthly Ops Cost < $20,000 > $10,000 0 = Monthly Ops Cost > $20,000 **(plug in real $/FTE levels)**				
Operations Costs (other)	**(note: factor in the data center, network, communications, disk storage, etc. costs)**				
Total					

c. Benchmarking

Concurrent with the assessment, benchmarking within the PSO industry (outside if warranted) of similar "best practice" applications should be conducted. Use the Application Assessment Scorecard to serve as the basis for evaluating other alternatives. This is very similar to performing a "buy vs. build" analysis as discussed above in *Section V. A. Buy vs. Build Decision*. Include other Power Systems Operator's applications as well as known vendors. The intent is not to select a specific application from a specific vendor, but to objectively evaluate your own application's fit and performance versus other similar applications in the market. Other alternatives that may be considered are application outsourcing, application leasing/hosting, and business process outsourcing. In addition, there are many hybrid solutions that would include salvaging component parts and building new, or salvaging/purchase/customize, etc. It is important to have both operations and IT resources involved in the benchmarking.

d. Alternative Analysis and Recommendation

At the completion of the assessment and benchmarking, alternatives (maintain, buy, build, outsource, hybrid, etc.) should be compared and a recommendation for action made. The analysis will use the Application Assessment Scorecard that has been updated with other alternatives to compare the different approaches. A cost/benefit analysis for each viable approach should be taken. At this point in the analysis, the fundamental question that needs to be answered is:

Is the cost to maintain/upgrade the application and keep it current with business needs less than the cost to outsource or replace the application with a new vendor package, with an application procured from another PSO, or with a custom-built product?

This is a simple question, but requires complicated total cost of ownership (TCO), ROI, and/or IRR/NPV calculations to compare current operating and maintenance costs, lost revenue, lost productivity and opportunity costs, intangible image in the market place costs, speed to market, etc. with the TCO of a replacement system or outsourcing. See above *Section III. IT Cost Management Best Practices.* Generally, the CFO within the PSO organization will specify the particular financial analysis that is required.

2. Remediation of a troubled application development project

Large, complex, multi-year application development or package customization projects consume significant personnel and capital resources, and are prone to a high rate of failure or abandonment. Many failures take a long time to be acknowledged by their sponsors and project teams. Most organizations believe that "failure is not an option", and continue to waste time and resources on unsalvageable solutions. Most senior IT and business managers do not specify the conditions that should be critically evaluated to determine the forward continuation of their projects once problems have surfaced. This lack of an "exit strategy" leads to runaway projects. The next sections address the actions to take to identify and respond to a failing application development project, as well as preventive measures to mitigate the risk of failure.

a. Problem Identification – Project Audit

Given the assumption that an application development or package customization project is in trouble – over budget, over schedule, solution not meeting the needs of its stakeholders, high internal/external staff turnover, changes in regulatory requirements or business direction, etc., the immediate priority is to perform a Project Audit. The Project Audit should be performed by

either an external third party, or by an independent Quality or Delivery Assurance body within the PSO. The purpose of the Project Audit is to objectively evaluate different aspects of the project to determine the true status and offer recommendations and an action plan for remediation. The Project Audit generally takes between 1 to 4 weeks to conduct, with additional time required to analyze data, make recommendations, and work with the project Sponsor and management team to identify action items. The team size, scope, overall project costs, length of schedule, complexity, geographic dispersion, magnitude of problem(s), project team cooperation, etc., will all determine the effort required to conduct the audit. The following highlights the key steps taken to conduct the Project Audit.

1. Project Audit team obtains Board or CXO[10] level Sponsorship and direction.
2. Announcement sent to Project Team regarding the audit: purpose, approach, schedule, required participation, and request for project documentation.
3. Project Audit team obtains and reviews Project Documentation.

b. Figure 21 – Project Audit Documentation Checklist

Document	Req.	Exists	Date Created	Owner	Rec'd
Statement of Work or Project Definition	☑				
Capital Funding Request/Business Case	☑				
Project Plans - Original, Modified and Current	☑				
Budget Spreadsheet	☑				
Changes of Scope	☑				
Staffing Plan	☑				
Team Organization Chart	☑				
Team member project expectations	☑				
Methodologies and Tools (SDLC, Project Management, Vendor Management, etc. and supporting tools)	☑				
Risk Management Plan	☑				
Quality Plan	☑				
Issues Log	☑				
Monthly Status Reports	☑				
Weekly individual team member status reports - all team members – minimum 3 weeks	☑				
Weekly team status reports - summarized – min. 3 weeks	☑				
Project correspondence to/from Sponsor, Operations Management, Boards, etc.	☑				
Signed deliverable acceptance forms	☑				
Team member task turnaround sheets	☑				
Issues Log	☑				

[10] "CXO" is here used to denote any of an organization's Chief Officers (e.g. CEO, CFO, CIO, CSO etc).

Document	Req.	Exists	Date Created	Owner	Rec'd
All Costs and Billing summary reports to date	☑				
All work products/deliverables to date - List each separately – for example: • Requirements Definition • Conceptual Design • Database Design • Technical Design • Infrastructure Design • Interface List and Specifications • Modifications List and Specifications • Application Development module Specifications • Unit, System, Integration and Acceptance Testing Plans, Scripts, Results • Performance Testing Plans, Results • Security Plan • Installation and Maintenance Plans	☑				

4. Project Sponsors, Oversight Board, Stakeholders, CXOs are interviewed to identify original solution expectations, issues, concerns, direction of the PSO, external risks impacting the project, budget constraints, etc.
5. Project team is interviewed – All Management (including vendors and third parties), All team leaders, All specialty functions (Technical architects, data architects, performance engineers, QA, etc.), Representative subset of team members from internal resources as well as vendor and third party (majority but not necessarily all).
6. The interviews are a critical component in the fact finding. They are structured around a number of focus areas, and are scripted for each project team role (i.e. team leader, team member, etc.). Not all interviewees will contribute data to all focus areas. It is important that a "safe" environment is established that enables open and honest disclosure (anonymity where possible).
7. The Project Audit team attends Project Status and issue resolution meetings, design, code and testing reviews, and reviews the application(s) where necessary. They may bring in specific technology experts to evaluate the functional and technical feasibility of the application.
8. Data is synthesized and evaluated in each focus area. Generally, summary red/yellow/green is identified for each focus area, with detailed description to follow. The detail should include the findings, areas of impact/risk, and recommendations to resolve.
9. Findings and recommendations are reported to Sponsor/Board/CXO; Project Team Management.
10. For recovery, action plans for recommendations are created, implemented and monitored; follow-up audits are conducted at predefined intervals. *(see next section)*
11. For project shut-down, project cancellation procedures are commenced. *(see next section)*

E. Phase II SAP HR/Financials Configuration Summary Findings

Project Start (Phase II): 6/22/04 **Planned Project End**: 4/26/05
Project Staffing: 46 **Project Budget**: projected $3,500,000 (Phase II)
Phase Description: SAP #.0b pilot implementation of FI, CO, PS, HR, SD, MM (data only)

a. Figure 22 – Example Summary of Project Audit Report

Review Category	Summary Rating	Rationale
Project Definition	**Red**	>30 days into Phase with SOW not complete (in progress). PSO has strong budget/schedule constraints and has not prioritized scope. Expectations have been set regarding completion dates and project costs in the absence of a resource leveled plan.
Sponsor Relationship	**Yellow/Red**	PSO Sponsor has expressed concern regarding leadership and management of project. The project team has not provided timely or regular status. The Sponsor does not feel that her organization's needs are being evaluated.
Planning & Tracking	**Red**	Incomplete Phase II plan – several non-integrated sub-plans under development – working almost 2 months w/out plan. Based upon projected implementation plan, the project is estimated to be 1.5 months behind schedule. Task actuals and ETCs are not being tracked.
Budget	**Yellow**	Estimated budget in place – not rationalized with leveled plan. Without plan in place, unclear as to true budget status.
Team Organization and Health	**Yellow/Red**	Both PSO and vendor staffing for Phase II was slow – impacting progress and team cohesion. Not all staff on board – PSO not committing all required resources. PSO is still lacking a technical architect, and approximately 7 developers. Vendor team well qualified. Project Management roles and responsibilities between PSO/vendor are unclear.
Methodology/Approach	**Red**	Team not following a standard SAP implementation methodology – each sub-team following own methods. No standards/procedures/templates infrastructure in place to support team. Project management methods for planning, tracking, issue management, status reporting, etc. either not in place, or ineffective.
Project Environment	**Yellow/Red**	Physical project environment is not sufficiently in place to support team (space, Ids, connectivity, software, etc). Team has not been given access to business users at Pilot sites to confirm requirements.

b. Project Remediation

The completed Project Audit Report summarizes all findings regarding the status of the application development/package customization project. It identifies problems, risks, and implications impacting the successful completion of the project in areas of schedule, costs, completion and quality of solution, and client/PSO satisfaction. Each problem is accompanied by recommendations and/or alternatives to mitigate the risk(s). There is a determination as to whether the project should be put on a recovery, redirection, or cancellation plan. With a cautionary/danger status illuminated by the Project Audit Report, the Board/CXO needs to answer the following questions to make such a determination.

- Was this project approved by an authorized Sponsor? Does the Sponsor still exist and still support the project? Does the new Sponsor support the project? Is it the right Sponsor?
- Does the Sponsor understand the complexities of the project and is he/she committed to ensuring its success by providing the required resources (dollars, people, equipment, schedule flexibility, and organizational support)?

- Are the Board and CXOs committed to ensuring the project success by authorizing the necessary resources ($/people/equipment) and providing organizational support?
- Is there a clear vision of the outcome of this project, and are objectives/goals identified, measured against and communicated?
- Are the expectations of the project by the Sponsor and/or the Board/CXOs realistic in terms of schedule, budget, and capabilities and quality of the solution?
- Is this project unique in that no other similar projects are underway/planned that are duplicating functions? If not, can it be incorporated into the other project?
- Is the project still anticipated to deliver the originally planned business value (i.e. cost/benefit)? Is the cost to complete the project budgeted in current/future budgets? Given the greater overall cost to complete the project, will it still produce a favorable ROI/IRR etc.?
- What is the earned value (not time elapsed/costs incurred) of the project's activities and deliverables?
- Is the project still in alignment with the overall current business strategy/direction of the organization?
- Is the enabling technology of the project currently operational? Can it be supported by the current IT staff? Is it already dated or obsolete? Is the technology in alignment with the architectural direction of the computing environment?
- Do the users see the value of the project? Have they been appropriately involved in the project? Will they continue to be? Will they accept and use the solution?
- Are there other alternatives to the solution being created, such as other application packages or other PSO implemented solutions? Have they been evaluated?

Given the large financial outlay of application development projects, there is a tendency to look backwards at the sunk costs and determine that an investment of this magnitude cannot fail, no matter what the cost to complete. That is an erroneous decision-making criteria, and often obscures the true viability of a project. All of the above needs to be answered to make the determination. Oftentimes, a high risk/high reward project is given two parallel paths going forward: (1) project recovery and (2) analysis of alternatives for redirection. If a decision to halt the project is taken, several steps should occur in the project close-down.

1) Project Recovery

To recover an ailing project, an action plan should be assembled and implemented to correct the deficiencies and put the project back on track. The action plan and the overall status of the project should be monitored regularly by the Sponsor and Board/CXO. To monitor the project going forward, a Project Report Card should then be established. It should contain specific measurements, or project vital signs that are tracked and reported out on a minimal bi-weekly basis to the Sponsor and Board/CXO (see *Failure Prevention* below for a review of the Project Report Card). There are various actions that could be taken to remedy a failing project, depending upon the circumstances. Below are general actions:

- Change schedule to allow more time to complete
- Increase budget to obtain additional resources and/or time

- Add and/or train resources to cover skill deficits (bring resources in from other PSOs, vendors)
- Add additional user/stakeholder resources
- Perform tasks in parallel
- Reduce scope of application
- Break solution into smaller, implementation releases and deliver less, more often
- Replace Sponsor
- Replace or add Project Management Team/PMO
- Alter approach and methodology of project

2) Project Redirection

To recover an ailing project, often a complete redirection is required. This may involve: (1) purchasing an off-the-shelf package to replace an application development project[11], (2) selecting an alternative package to the current one that is being configured/modified, (3) scrapping a package (or part) to undertake application development. Some decisions are made to immediately halt the failing project and review the alternatives for redirection, and others allow for the continuation of the project but seek a parallel analysis of alternative solutions. In either case, the project team should undertake a thorough evaluation of the alternatives before commencing and possibly making another mistake to correct the first one. They should follow a similar approach as outlined above in the *Application Assessment* and *Benchmarking* sections.

Once the analysis of alternatives is completed, the project team should present its findings and recommendations to the Sponsor and Board/CXOs to obtain approval of the new approach/solution, budget and schedule, and resource requirements.

In addition, there should be an attempt to salvage usable components from the failed project to accelerate and leverage the new project. Critical team members and users/stakeholders should be retained for continuity, and under-performing or inappropriately skilled team members should be reassigned. Remember that any redirection that involves new, external parties (software vendors, third party integrators, other PSOs, etc.) will require new contract negotiations and definition of terms and conditions. This process needs to be accounted for in the new schedule, and could be substantial in elapsed time.

As in the *Project Recovery* section above, a Project Report Card should be created, tracked against and reported out to the Sponsor and Board/CXOs on a bi-weekly basis to ensure that the new project approach/solution stays the course.

3) Project Cancellation

Some projects are not able to be, or shouldn't be saved or redirected. Once determined, a Cancellation Plan should be put in place by the Sponsor and Project Management team. This

[11] The ISO New England Board chose this direction after two years of work on implementation of the ISO's proposed CMS/MSS market design. The CMS/MSS design was scrapped in favor of an existing market platform that was in operation in PJM. ISO New England implemented its Standard Market Design (SMD), which was modeled after PJM's design, on March 1, 2003.

plan should strive to minimize the impact to the user/stakeholder community, as well as the project team members. The Cancellation Plan should include the following activities:

- Create the plan
- Communicate the cancellation and/or redirection (privately to stakeholders/publicly to others)
- Consult with the Legal Department regarding contracts
- Consult with the HR Department regarding team personnel issues
- Salvage usable project components (contracts, requirements, design, test data, plans/estimates, equipment, software, testing environment, facilities, etc.)
- Conduct a sunset review with the team to gather lessons learned
- Reassign team members
- Dismantle facilities
- Redistribute equipment (hardware/software, etc), recycle, return to leaser, sell

c. Failure Prevention

Most projects can be planned, managed and monitored to prevent failure. Many risks can be identified and mitigated but unforeseen internal and external events can not always be avoided. These events may force a redirection or cancellation of the project. Such events may include:

Internal:

- Change in Business Direction or Strategy
- Change in financial status
- Change in Sponsorships, Boards, CXOs
- Competing priorities
- Merger/Acquisition

External:

- New or revised Regulatory requirements (i.e. SMD)
- Market restructuring and new/different competition
- Natural or unnatural disasters (i.e. Blackout)
- New or improved vendor/PSO solutions

By following many of the best practices outlined in *Section VI. Appendix 1: PSO IT Best Practices Guidelines*, most projects can avoid failure. In addition to those things discussed such as proper *IT Organization and Culture, IT Strategic Planning and Portfolio Management, Project and SDLC Methodologies, Vendor Evaluation and Management, Problem Resolution and Management, and Root Cause Analysis,* accurate and timely status reporting, communicating, and monitoring is essential. Regular project auditing as discussed above should be conducted, even if the project is not known or suspected to be failing. The larger, higher risk/reward projects should be audited on a regular basis and/or in conjunction to project phases or milestones (i.e. end of requirements definition).

d. The Project Report Card

As discussed above, a Project Report Card should be established. This should be completed before the project starts, and communicated during the project kick-off. The Project Report Card should contain specific measurements, or project vital signs. These measurements are

accompanied with variances established by the project Sponsor and Board/CXO to objectively identify the status of each. Each variance is then assigned a point value, with the higher points indicating a more serious project problem (note: alternatively, each variance could be assigned a red/yellow/green indicator like above for danger/caution/on-track instead of points).

The Sponsor and Board/CXOs establish the overall project thresholds. These thresholds indicate a combined scoring of the different measures into the three red/yellow/green (danger, caution, on-track) categories. For example, the combined scoring across all measures:

On-track/Green = 0-10 points	No action required
Caution/Yellow = 11-20 points	Action required to mitigate
Danger/Red = 21 points and higher	Project in danger of failure; decision to recovery/end

It is very important to identify the Danger (red) threshold at which time the project would be in serious trouble and should be evaluated for project shut-down or recovery. There should be a previously agreed upon action plan that could be implemented if the Caution or Danger threshold is reached. If the project is in Caution mode for weeks or more, the project should automatically be moved to the Danger threshold.

On a monthly basis (bi-weekly for high risk or already in danger), the project management team should identify the status for each measure, assign and tally the points to create a single score. A completed Project Report Card would have a summary section for a total combined score, measurement categories and sub-total scores, and a detail section that lists the measures, variances, points available, and actual points (scores). Action items should be identified to remedy any at-risk areas (i.e. extend schedule for new mandatory requirements from the Stakeholders). The completed Project Report Card and supporting information and action plans should then be presented to the Sponsor and Board/CXO. Actions requiring Sponsor and/or Board/CXO approval should be reviewed and addressed promptly. Failure to make timely decisions by the Sponsor/Board/CXO will render the Project Report Card and communication process ineffective.

Trends between reporting periods should be identified. It is useful to use ⇧⇩symbols next to each measure score, sub-total, and overall combined score to show movement from the prior reporting period. See Figure 25 for an example Project Report Card.

e. Figure 23 – Example Project Report Card

Measure	Variances	Points
Project Definition		
Triple Constraints: Budget, Schedule or Scope rigidity = # of Constraints	0 1 >1	0 2 4
Approved Work: All work has approved Project Definition/SOW or Change of Scope document	• PD/SOW/COS is signed • PD/SOW/COS written, being finalized, and project less than 30 days old • No signature & project more than 30 days elapsed, or PD/SOW/COS is not discussed	0 1 2
Contract Status: All vendor Contracts accurate/current = $ amount of unsecured work	< $100,000 $100,000 to $250,000 > $250,000	0 1 2
Sponsor Relationship		
Sponsor Perception: Sponsor is satisfied with work = % of deliverables accepted according to acceptance timeframe	> 90 % 75% to 90% < 75 %	0 3 6
Sponsor Responsibilities: Sponsor meets the following responsibilities: 1. Attends 90% > status meetings 2. Resolves issues within agreed upon timeframe >90% 3. Provides resources according to project schedule >90% 4. Accepts deliverables within agreed upon timeframe >90% 5. Communicates project status with Board monthly	5 items 4 items < 4 items	0 3 6
Planning & Tracking		
Schedule: Actual vs. plan = % difference in days	< 5% 5% to 10% > 10%	0 2 4
Milestone/Deliverable: Actual vs. plan = % milestone/deliverable dates missed	< 5% 5% to 10% > 10%	0 2 4
Unresolved Issues: Issues that are outstanding and may impact project cost/schedule/quality = # of issues that have >5% of total project cost impact	0 0 to 2 >2	0 2 4
Budget		
Budget: Actual vs. Estimated = % over or under budget	< 5% 5% to 10% > 10%	0 2 4
Cost to Complete: Actual vs. Estimated = % difference	< 5% 5% to 10% > 10%	0 2 4
Team Organization and Health		
Staffing: Actual vs. Planned = % difference	< 5% 5% to 10% > 10%	1 3 5
Team Health: The following : 1. Absenteeism < 2% 2. Training requested is received 90% 3. Project expectations written/reviewed 4. Status meetings with Project Manager held 95% of time 5. Turnover < 5% 6. Staff issues resolved quickly 7. Overtime hours < 10%	6-7 items 4-6 items < 4 items	0 2 4
Methodology/Approach		
Standards: Ensure that methodology is being followed = % of work products/deliverables that follow methodology standards	> 90 % 75% to 90% < 75 %	0 1 2
Business Functionality Issues: = # of unresolved business functionality issues that have >5% of total project cost/schedule delay impact	0 0 to 2 >2	0 2 4
Technical Issues: = # of unresolved technical issues that have >5% of total project cost/schedule delay impact	0 0 to 2 >2	0 2 4
Project Environment		
Environment Resources: (equipment, testing environment, etc) Actual vs. Planned = % difference	< 5% 5% to 10% > 10%	1 3 5
Risk Management		
High Probability/High Impact Risks: = # of risks that have >10% of total project cost impact; or ability to stop project (loss of funding or Sponsor, change in corporate direction)	0 0 to 2 >2	0 3 6

F. What should be considered the normal lifespan of grid management applications and systems?

It is very difficult to determine a precise estimated life span of applications and infrastructure used by Power System Operators as the applications have been implemented at different times and the specific technology life spans are subject to various factors. However, it is possible to provide some general guidance on the topic and provide recommendations for systems implementation that could extend the life span in some cases by limiting the risk of obsolescence. The recommendations that are listed in *Section III.C.* regarding the implementation of PSO systems will reduce the cost of the implementations and extend the life of the applications.

1. Justification for Application Replacement

Projects to replace applications are generally very costly, require a significant expenditure of the PSO employees' time, and have a significant impact and risk on the PSO's operations. Therefore, it is very valuable to extend the life of the applications for as long a period as is possible. In general, applications and infrastructure should not be replaced unless the business needs and requirements are not being met. These requirements can take various forms are described as follows *(detailed Application Assessments are discussed in Section V.B.c.1.)*:

- The application no longer meets the functional requirements of the business. This can occur because the business process has changed or new requirements have been introduced due to changing business situations (e.g. an ancillary services market is introduced and the settlements system is not capable of addressing the new requirements) or reliability requirements (e.g. faster state estimator calculations or wider EMS monitoring footprint).
- The existing application or infrastructure component is too costly to maintain compared to the implementation of a new solution. A discounted cash flow model of the costs to maintain the application should be prepared. This should be compared to a discounted cash flow model of the cost to implement a new solution plus the cost to maintain the new solution over time. There are times when this analysis will yield results that justify the implementation of a new application. However, this scenario is infrequent unless the application depends on hardware or software that has become technically obsolete and, as a result, the cost of maintaining these components has become exorbitant.
- The application or infrastructure has become technically obsolete. This situation can occur when proprietary hardware and software platforms are required to run the application. As vendor hardware lines are replaced with newer offerings, the previous hardware generations are generally abandoned. Replacement components become difficult to acquire and the maintenance cost of the hardware becomes very high. In some cases, it becomes impossible to procure a maintenance contract. This is a situation that the PSO must avoid. No PSO system should be operated where a maintenance contract is not in place. Similar, some software platforms that the applications are built upon become obsolete as replacement products are brought to market. In many cases, it becomes impossible to procure software support and maintenance on these software components. This is also a situation that the PSOs should avoid by planning out their replacement projects. It is sometimes possible to

hire knowledgeable personnel to support these software components but this should be seen as a short term strategy only.

- The performance of the system has become too slow to process the information or perform the analysis within an acceptable period of time. Generally, if no changes are introduced into the environment, applications do not perform slower over time. However, the performance of many systems has degraded as the size of the data or the amount of analysis has increased leading to unacceptable performance. For example, the increase in the number of SCADA telemetry points or the desire to analyze an additional number of contingencies in a shorter period of time may result in performance problems. These performance degradations can sometimes be offset by hardware performance improvements but that is dependent on the degree to which the application can run on various hardware platforms.
- The technical architecture of the system has become inconsistent with the rest of the PSO technology environment. PSO IT organization's can reduce their support costs and raise their performance by maintaining a standardized technical environment. When systems become inconsistent with their internal standards, the support cost often rises and performance may suffer. In addition, the ability to make changes and integrate the applications with other applications is usually lower when a different architecture is employed since it is harder to maintain a knowledgeable staff. This scenario, however, is rarely sole justification for replacing an application as the incremental support costs rarely offsets the cost to implement a new application. PSOs should develop a technology architecture roadmap and design their applications accordingly to minimize the chance of these architectural differences.
- The vendor supporting the application has become financially unviable (e.g. bankruptcy) and support for the application can not be procured. Many of the applications used by the PSOs are critical to the organization. Therefore, the PSOs need to ensure that the proper level of application support is available from the vendor or the PSO has staffed their organization with skilled and experienced people to internally support the application. Access to source code is essential to internally providing the application support. When vendor viability is questionable, steps should be taken to ensure that source code is placed in escrow in the event of vendor bankruptcy

If it is determined that the current application(s) do not meet the business needs and requirements as defined above, the PSO will need to decide whether to make significant changes to, or totally replace the system. The process that is discussed in *Section V. A.* to determine a Buy vs. Build strategy should be followed at this point. The following sections address the six major PSO application categories and the specific situations that may shorten the life cycle of the applications. For purposes of this discussion, short term is considered 1-2 years, medium term is 3-5 years, and long term is over 5 years.

2. Market Applications

For many PSOs serving as Market Administrators, their Market Applications are relatively new, having been implemented recently as part of the implementation of their market. Therefore, it is unlikely in the near term that these applications will be subject to any of the triggering events described above in *Section V.D.1.* that would compel the PSO to replace the systems. As the specific markets mature, however, the PSOs will introduce new services and markets that will

require additional functionality that is not currently in use. Some of the independent software vendors have included this functionality in the software, although it may not currently be used. The PSOs will need to evaluate the degree to which this embedded software functionality addresses the business requirements for supporting the new services and markets. If there is a gap between the software functionality and the business requirements, the PSO will be faced with the decision of either making a significant investment in the software to address the gap or to look for a new solution where the software functionality matches the business requirements.

PSOs that have developed their market applications internally usually have a higher degree of control in modifying the applications to meet evolving business requirements. However, this does not mean that these modifications are simple and inexpensive. The project to implement the software changes to support new market functionality in internally developed software is at least as complex as packaged software and, in many cases may be more complex.

The Settlements systems and systems that provide settlements-related information to market participants will need to undergo significant changes to support the new services and markets, and to address the desire of the market participants to have better and timelier access to settlements data. PSOs should plan to make significant investments in these systems throughout the near to medium term.

PSOs that have recently implemented energy and ancillary markets need to assess the potential impact of a significant increase in the number of energy bids and transactions. As market participants and their trading systems become more sophisticated, they will begin to increase their number of bids. The technical infrastructure that supports the Market Applications and the applications themselves will need to be sufficient to handle this additional volume. Otherwise, they will suffer from performance problems and face premature technical obsolescence.

3. Open Access Transmission Service Applications

Most of the Open Access Transmission Service applications at PSO's have been commercially available for years. Thus, the software is very mature and is generally very stable. One functional item that PSO's should investigate is their ability to dynamically monitor transmission stability issues in real time through their existing software. In general, though, it is not anticipated that there will be significant additions to the functional requirements for this software that will necessitate changes through the medium term. PSOs will need to assess the potential technical obsolescence of these systems since they may have been built on proprietary hardware or software platforms.

4. Short-Term Transmission System Reliability Applications

The Short-Term Transmission System Reliability applications are arguably the most business-critical applications to the PSOs. The engineering algorithms have been in existence for many years and the systems are proven technology. These algorithms that are foundational to the Reliability Applications are not anticipated to change significantly in the near term; however there are several new capabilities that may require changes to the Reliability Applications or may require additional systems that are integrated with the Reliability Applications. Some of these new functions are as follows:

- The ability to perform critical facility loading assessment via the use of Line Outage Distribution Factors.

- The introduction of new RTU devices that capture additional data types and / or a large increase in the number of RTU's located in the field.
- The ability to send and receive Network Model updates automatically between the Control Areas and the RTOs and ensure that they are kept synchronized.
- The ability to perform Real-Time Thermal Capability assessment based on prevailing pre-load and ambient or dynamic field measurements.
- The ability to receive real-time data from external entities (e.g. other PSOs) and fully incorporate the information into the Reliability Applications.
- The ability to perform Real-Time Short-Circuit assessment based on prevailing network and generation.
- The ability to perform dynamic security assessment using transient & voltage stability limits.
- Improved visualization techniques and intelligent software to analyze conditions, prioritize issues, and recommend actions. These technologies should address some of the human factor issues that are currently affecting the control room operators.

It may be possible to incorporate or introduce these new features and capabilities into the existing applications without fully replacing them. Additionally, it may be possible to develop new applications that provide these features and integrate the new applications with the existing applications so that they can take advantage of the new calculations. In any event, the PSOs will need to be prepared to make significant investments in these applications in the near to medium term if they plan on introducing and utilizing these new capabilities. During their technical planning processes, the PSOs should develop a plan that incorporates the anticipated technical obsolescence with the implementation of the new features. This will help the PSOs implement systems that have a longer life span.

5. Transmission Planning

The Transmission Planning applications are not expected to see significant changes to their functional requirements in the near term. The applications have been in existence for a long while and are very stable. These applications generally have a lower reliance on data center capabilities and are thus, less subject to technical obsolescence. Generally, the PSOs should not need to make significant investments in these tools in the medium term though they should evaluate the increased use of P-V (Power Voltage Relationship) and V-Q (Voltage Reactive Power Relationship) analysis for both long-term and operations planning.

6. Corporate Administration Applications

Many PSO organizations have implemented package solutions from large independent software companies to address their Corporate Applications, namely Accounting, Compensation & Benefits, and Human Resources. These software solutions offer all of the functionality that is generally required by the PSOs. In cases where the PSO has not implemented all of the modules available, it is a reasonably straightforward process to contract for and implement the remaining modules that have yet to be implemented. These packages have strong maintenance and support from their vendors who provide upgrades on a regular basis. They are built on non-proprietary architectures so the risk of technical obsolescence is low. The software industry that provides these applications has already gone

through a consolidation and reduction, thus the risk of vendor viability is reasonably low for the Tier 1 and 2 vendors.

Many PSOs have not implemented robust Customer Information Systems (CIS) or Customer Relationship Management (CRM) systems. This is a decision that the PSOs will need to make in determining whether there are compelling reasons to pursue this path. Some PSOs have recognized that this system is a critical component of addressing market participant and customer needs and are actively pursuing the implementation of a CRM solution that will enable them to improve their customer responsiveness. For PSOs that have not made this determination, they should consider this in their next planning cycle for the near to medium term.

7. Market Monitoring

Market Monitoring applications consist of a collection of tools used to monitor the market participants bids and the general functioning of the energy markets. Typically, these applications are run after the market closes to ensure that there has been no anti-competitive behavior. As such, they have not required as much infrastructure as many other PSO applications, do not have the same operational performance requirements, and are simpler to modify. These analytical applications are not expected to have a significant number of new functions. However, it is known that a greater level of bid data analysis will need to be performed by the market monitoring applications.

8. Technical Infrastructure

Each of the components in the PSO Technical Infrastructure (as defined in *Section II. H.*) has a distinct life cycle and is subject to technical obsolescence as well. These life cycles are generally known given the current technology capabilities of the equipment, but could change as the technologies evolve. The following guidelines can be used for the expected life cycle for infrastructure components:

- Mainframe and servers have an average life span of 3-5 years. PSO organizations should plan on replacing these items according to this time line.
- Storage systems have an average life span of 3-6 years. PSO organizations should plan on replacing these items according to this time line
- Routers (Wide Area Network) and Switches (Local Area Network) have an average life span of 4-6 years. PSO organizations should plan on replacing these items according to this time line.
- Remote Terminal Units (RTUs) have historically had an average life span of 8-12 years. However, as PSO organizations look to implemented a "smart electric grid" by capturing additional information about the real-time condition of the grid, they will need to begin a program of replacing a large number of the RTU's that are in the field. These newer devices may be 100 times more costly than existing units and will require significant expenditures in network equipment and network management tools to be able to manage the expanded technical environment.
- Network Management, Systems Management, Network Operations Center, Help Desk Tools, Network Tools, and Network Security software often have an average life span of 5-10 years as these software products are generally upgraded on an annual basis where new functionality is added.

- Laptops / Desktops have an average life span of 3-4 years. PSO organizations should plan on replacing these items according to this time line.
- Voice based infrastructure (e.g. PBX, Voice mail) have an average life span of 6-10 years. PSO organizations should plan on replacing these items or upgrading them according to this time line.

G. What are the issues associated with the limited number of vendors who supply reliability management products and how can the risks be mitigated?

The limited number of vendors in the reliability management and market administration product sectors may not be an issue, but the potential over-reliance on one or all of these vendors by a PSO may introduce an unacceptable level of risk. The following sections will look at the potential issues involving vendor dependency, and the strategies to be explored to mitigate the risks.

1. Limited Number of Vendors

The limited number of vendors who supply reliability management and market administration products is not a unique challenge to the PSO industry. Many industries do not have commercially available solutions to support their key business processes, and others are faced with a choice between one or two vendor products. For the Corporate Applications that are addressed by the more established Enterprise Resource Planning (ERP) commercial software vendors, the industry has seen the consolidation of its vendors over the last 10 years resulting in the "Big 3" (SAP, Oracle, and PeopleSoft) domination of the market, even where other solutions/vendors are available. This has not led to less competition in the marketplace, but has arguably led to greater competition. It has forced these vendors to improve their products, services and value (cost/benefit). There is no indication that a small number of vendors in the reliability management and market administration product sectors can not be financially successful and provide high quality products.

At greater risk is the potential for further consolidation of the remaining reliability management product vendors. Any merger or consolidation activity that results in a single vendor product solution would eliminate competition and create potential vendor dependence for those PSOs without alternative solutions. Lacking alternatives, a PSO could face potentially higher acquisition, maintenance and upgrade costs, slower product development, unsupported solutions or solutions that are out of alignment with their technical direction. Currently, there is no indication that this will happen in the reliability management product sector.

2. Vendor Dependency

Many established PSOs have a mixed application portfolio that contains a range of products along the "Buy vs. Build" continuum. In addition, many of the applications and/or components from the "buy" side are provided by different vendors. With a diversity of externally sourced applications and in-house developed applications, these PSOs have balanced their risk of single sourcing from one vendor. They also have generally built up their internal technology capabilities to provide an alternative to package solutions if necessary.

The challenge is greater for those PSOs who have out-sourced much of their application development and/or architecture skills and have become reliant on vendors and third party integrators to maintain and upgrade their applications. Newer PSO market entrants who are establishing a new technology infrastructure and have more commercially available products to choose from, but less in-house technical expertise to build custom solutions face a different challenge. They may become too reliant on vendors in general. Also at higher risk are those PSOs who have opted for single vendor solutions to handle all of their critical reliability management needs. As software vendors open their system architectures, thus promoting

interoperability with other software solution, the PSOs vendor dependency (and concomitant vendor risk) is reduced.

a. General Vendor Dependency

Those PSOs who are/could become overly reliant on vendor solutions *may* be faced with the following challenges:

1) Organizational Issues

- Higher costs for maintenance, modification, integration, upgrades
- Inability to quickly meet changing business or regulatory requirements
- Erosion of internal technical capabilities resulting in further vendor reliance
- Poor internal IT image compelling operations to begin decentralizing IT

2) Technology Issues

- Heterogeneous, complicated, and expensive technical infrastructure
- Closed/proprietary technologies vs. open architectures
- Aging technology that is no longer supported by hardware vendor but is required to run the applications
- Too frequent or infrequent patches, upgrades
- Integration challenges

b. Single Vendor Dependency

Those PSOs who rely on a single vendor for all of their critical reliability management and market administration technology solutions may face the same challenges as those who are overly reliant on technology vendors in general. However, they *may* face the following vendor viability and changing strategic direction risks as well:

- Financial instability and/or target of acquisition
- Initiator of consolidation and potential spin-off or sale of product line
- Shift in product/industry priorities
- Failure to invest in R&D and new releases or upgrades
- Tendency to reward larger customers by gearing upgrades/releases around their requirements

3. Mitigating Vendor Dependency Risks

Recommendations to mitigate the real or potential risks of PSO dependency on one or more reliability management and market administration application vendors are briefly discussed in the following sections.

a. Balanced Application Portfolio

As discussed above, PSOs manage an application portfolio that contains a range of reliability management products that fall along the "Buy vs. Build" continuum ("Bought vs. Built"). To

balance their risk, the PSO should consider a balanced approach to their portfolio. While it may not be financially feasible to "build" more than "buy", it may be possible to buy best-of-breed applications/components from different vendors. In this way, the PSO does not have a single source dependency. (This implies that different vendor products are compatible – see next section on Open Systems Architecture Strategy.) PSOs that currently have vendor dependency problems should reevaluate their application portfolio and create an IT Strategy and Plan to migrate to a balanced portfolio approach if the cost, functionality, and ability to maintain the applications is not reduced by this strategy.

b. Industry Standard and Open Systems Architecture Strategy

Regardless of vendor dependency, all PSOs should be moving towards an industry standard common architecture. A common architecture will guide vendors to adapt or migrate their solutions to work on a common platform. The Reference Architecture designed by the ISO/RTO Information Technology Committee is a great start in establishing such. By defining different best practice technologies for the six domains (security, application, data, infrastructure, platform, and redundancy), the ISO/RTO Information Technology Committee (IRC ITC) has established a framework and direction to which reliability management application vendors (others as well) can adapt their products. In addition, by building a consortium that recognizes the needs of the entire industry, new product offerings should address a wider spectrum of requirements and, thus, require fewer changes and minimal customization.

PSOs should adopt and encourage the use of non-proprietary technologies that use open standards across the above mentioned six domains. Not only will this lessen the dependency on specific vendor solutions by enabling choice, it also allows for easier and less costly interoperability and data exchange.

The ISO/RTO Information Technology Committee (IRC ITC) mentioned above, in collaboration with EPRI and the major product vendors have made great strides in the development and/or adoption of data standards (CIM/CME), as well as data exchange message standards that will allow for vendor independent solutions such as SCUC. This Market Standards Collaborative begins to demonstrate the value of industry standards and vendor collaboration in driving to consistent and cost effective solutions.

c. Requirements and Design Documentation

PSOs can ease their reliance on application vendors somewhat by creating and maintaining current business/ technical requirements and design documentation of their reliability management (overall operations) functions. These documents should detail the business processes and business rules that are supported by the application(s). In addition, the database design, system architecture design, and configurations, modification, and interface specifications should be maintained as well. Test plans, scripts and training material are also essential. By maintaining such "blueprints" and specifications, the PSO retains the intelligence of the vendor application, if not the code. Such intelligence better positions the PSO to understand the impact of modification requests and/or upgrades to their current application, thus, allowing better financial and technology decisions. In addition, if the PSO needs to replace all or parts of the application(s), they can accelerate the selection, requirements, and design process; reducing the time to market, costs, and risks. When determining its application requirements, the PSOs should not engage software product vendors to assist in this process as it may become biased by the functionality that is already contained in the vendor's product. Independent parties should be

used to assist in the requirements gathering process to ensure that the integrity of the process is not compromised.

d. Investment in IT skills

Many PSOs have reduced their in-house Information Technology skills by contracting out particular IT functions such as application development, database design and management, or data center operations. The decrease in staff, as well as erosion of specific technical skills results in an increased dependency on product vendors and systems integration consultants to develop, maintain and run critical reliability management applications. While it may not be in the strategic or financial interest of the PSO's IT organization to fulfill all of these technology needs, they need to evaluate the cost/benefit/risk of in-house vs. external product/service provision. To minimize vendor dependency, they will need to invest in some in-house technical experience with these critical applications to be able to triage operations problems and facilitate and manage application modifications, interfaces and upgrades.

e. Vendor Partnership

PSOs can ease the risks of vendor dependence by developing long-term, strong partnerships with their critical reliability management applications vendors that are based upon trust, shared risk/reward and mutually understood goals and objectives. Clearly defining the roles and responsibilities of each party and establishing service level agreements (installation, operations, and maintenance) that are fair and achievable aid in this partnership. Open communication and regular monitoring and adjustment of SLAs (Service Level Area) are also important. By having a vendor that is only financially-driven and not committed to the overall success of the PSO, the PSO will not establish the level of partnership that is sustainable in the long term, one that will grow with its evolving needs.

H. What is the impact in terms of dollars and time of excessive delays in decision making caused by FERC, the market participants, or other critical stakeholders when new technology is being implemented?

Project delays as a result of participant and Regulatory decision making are an inevitable issue of any new PSO technology implementation, particularly those that involve new regulations, market designs, market rules, technology standards, processes and data, integration needs and organizational changes. The PSO can anticipate and manage the impact of delays by structuring the technology project into manageable releases and project phases, and by using standard Project Management and SDLC Methodologies (see Section *VI. Appendix A: PSO IT Best Practices Guidelines*) that plan and account for critical path bottlenecks, decision making gaps, and the design of parallel tasks that may minimize project downtime.

Proper governance structures within and surrounding the project with well defined and executed reporting, monitoring, and issue management processes can facilitate speedier decision making. Additionally, a well defined Change Control process administered by the Project Management team will objectively identify, analyze and report the impact (schedule/costs) of decision making delays (as well as other factors that may impact the cost/schedule/scope of the project).

1. Project Planning

Managing project delays starts with the overall structure and approach to the technology implementation. Planning the project into small releases of functionality that can be delivered in shorter timeframes is the premise behind Release Planning. Ensuring that a Requirements Definition and subsequent Solution Design is in place before package configuration/customization or application development begins is critical in "freezing scope" and minimizing large, costly changes to the solution.

a. Release Planning

At the onset of the project during the Planning Phase of the Systems Development Life Cycle (SDLC) methodology, the PSO, Regulators and Stakeholders should clearly articulate the objectives, scope and outcomes of the technology implementation. They should work together to chunk the solution into smaller, more manageable pieces that can be implemented in shorter timeframes, with less risk. Undertaking "big bang" implementations that are characterized by multiple systems, complicated and abundant interfaces and data conversions, and many vendors that span many years (i.e. greater than 2) is not only risky, but more difficult to manage and adapt to changing requirements. Failure is much higher for these types of implementations, and even when eventually implemented tend to be much costlier and not responsive to new market rules.

Release planning should be applied to any large technology implementation, regardless of whether it is a package/configuration, package/customization, or application development project. The releases have discrete functions identified, and are ordered by evaluating many factors such as system/data dependencies, value to the stakeholders and PSO, and mandatory regulatory changes required by a certain date. The ideal release timeframe is three to nine months for detailed design, modification/build, testing and deployment. Earlier releases tend to take longer than subsequent ones. Releases overlap in the schedule, where one release may be in testing, some in development, and some in the detailed design phase. While many vendors will try to persuade the PSO to go "big bang" by recommending against releases because of potential

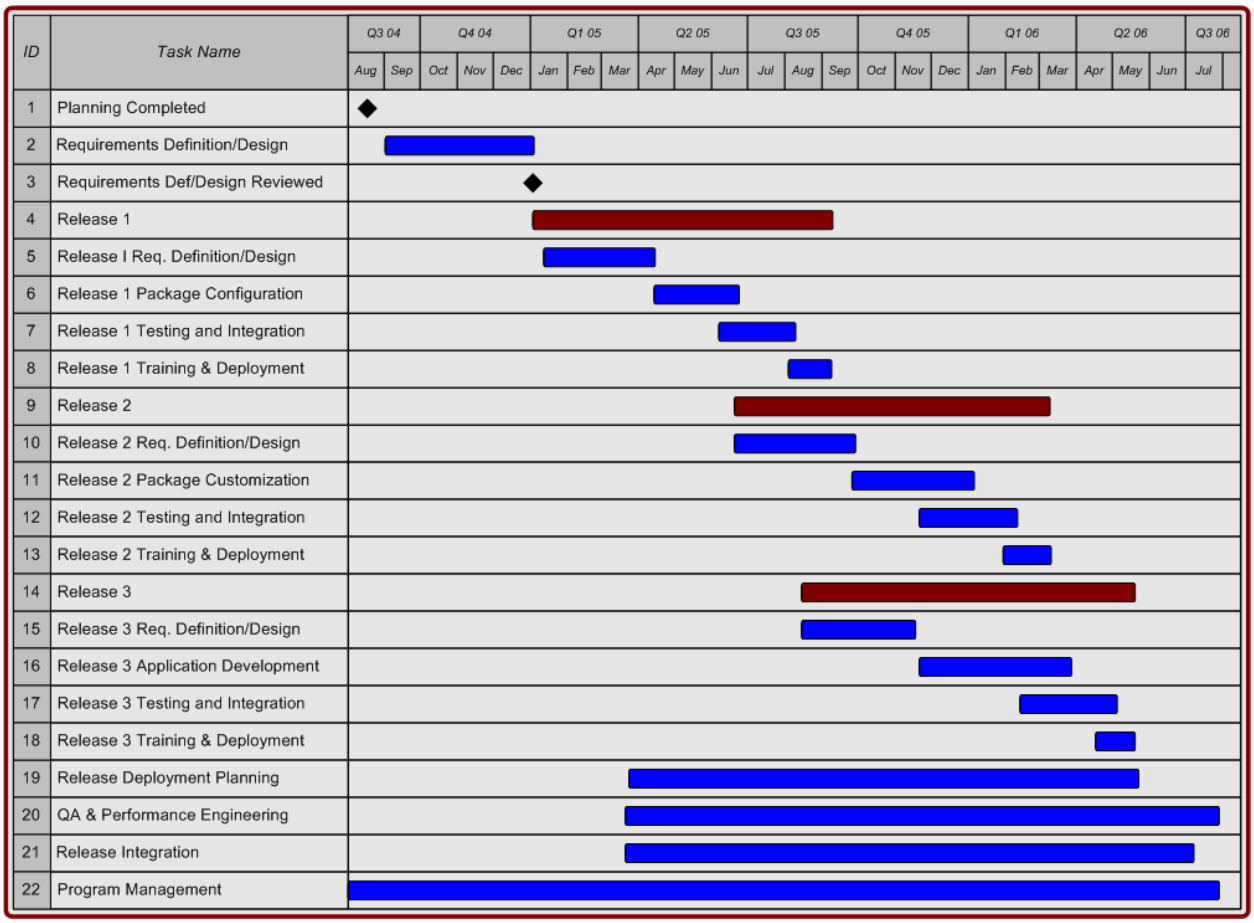
technical decoupling difficulties (and fear of competitor products being substituted for different sub-systems), release planning should be pursued until proven infeasible.

By implementing releases, or pieces of the entire technology, specific decisions required from Regulators or Stakeholders that may have long resolution timeframes but *do not significantly impact the overall design of the solution* can be deferred to future releases. Note of caution: Many market design or market rule decisions must be defined before any release is implemented, because the amount of rework could be great, cascading across multiple releases.

At the conclusion of Release Planning (which occurs at the end of the Planning Phase), a multi-year Release Plan Roadmap should be produced. Broken into a monthly or quarterly timeframe, the Release Plan Roadmap should show the subsequent phases of the SDLC required before work on specific releases starts, as well as each release broken into each of its project phases. Dependencies between releases should be identified and detailed, as well as the assumptions used to define the releases. Each release should have a detailed definition of the scope and functionality of each release, as well as the planned technology solution and estimated costs/benefits and resource requirements. This should be presented to the appropriate Regulators, Boards and Stakeholders and adjusted where necessary. Sign-off by all should be obtained before starting the next phase(s).

As mentioned in the opening paragraph of this section, project delays as a result of the market and regulatory decision making process are inevitable. As changes to market rules, exceptions, and grandfathered agreements are made during the project, it is not unusual that additional software releases will be required during the project. Each new software release could easily add two to four months of additional time to the project schedule. This additional time usually occurs when the project team is at its maximum size so the additional project cost resulting from these changes is generally very large. The PSO organizations should work with the regulatory agencies to ensure that all parties understand the repercussions of changing these critical elements once the project has reached the design phase.

b. Figure 24 – Representative Release Plan Roadmap



c. Requirements Definition/Solution Design

If a release-based approach is followed, there will be two levels of Requirements Definition/Solutions Design. The first level includes the big picture specification of the entire technology solution and is started at the end of the Planning Phase of the project referenced above. Major scope and business/market rules are identified and resolved during this phase(s) (some SDLCs have separate Requirements Definition and Solution Design phases), as well as more detail around internal/external interfaces and data conversion needs. Technical infrastructure components (i.e. database, security, server configuration, storage, etc) are specified (if not previously due to long lead time required). Facility considerations are evaluated, as well as future capacity requirements and system performance targets.

The specific, actionable requirements will be defined during the Requirements Definition/Solution Design phase for each release. These requirements will define the configuration criteria or modification needs for a package solution, or the programming specifications for an application development project. In addition, detailed design for system interfaces and data conversion that affects the specific release with be completed.

At the conclusion of each of these phases, the Requirements Definition/Solution Design should be reviewed with the appropriate Regulators, Boards and Stakeholders and adjusted where

appropriated. Concurrence and sign-off is important before the project can proceed to the next phase. By doing this, project delays that may occur during development because requirements were not "nailed down" should be minimized. In addition, any delays that occur will be less costly to the overall budget, as only project resources involved in the analysis and design will experience delay (less costly than having many vendors and in-house development staff sitting idle and consuming the budget).

2. Project Governance

In addition to having the right approach and SDLC methodology that incorporates Release Planning, it is important to have the correct Governance structure and processes in place to execute and oversee the management of the project (see Section *VI. Appendix A: PSO IT Best Practices Guidelines*). In simple terms, governance involves determining what the right things are, and ensuring that they are done right. It is comprised of the organizational bodies and roles and responsibilities of those responsible for ensuring a project success, and the processes that these bodies follow.

a. Organization Design

To avoid repeating Section *VI. Appendix A: PSO IT Best Practices Guidelines* where IT Organization and Governance is discussed in more detail, the key points regarding governance bodies will be touched on. Below are some governance bodies and positions that provide direction and oversight to the strategy, planning, resource management, and execution of the technology project. Specific Regulatory committees or bodies are not included in this overview.

1) Joint Steering Committee/Board

A Joint Steering Committee (JSC)/Board consisting of internal PSO business and IT executives (CXOs), Operations, Finance and IT Directors, as well as key Stakeholders and Regulatory representatives should be established to provide the ultimate governance and oversight for the project. The JSC/Board should authorize the scope, budget, and schedule of the technology project. In addition, key market rule/design decisions should be reviewed and approved by them. The Joint Steering Committee/Board should meet monthly at a minimum, and be available to meet more frequently to resolve major issues and review key project milestones and deliverables

2) PSO Executive Management (CXOs)

Any significant technology project should be sponsored by the CEO/COO in conjunction with the Chief Information Officer (and/or Chief Technology Officer) to achieve greatest alignment between IT and operations. The CEO/COO authorizes the budget, schedule and scope of the project, as well as provides the resources ($/human/technology) and the priority within the PSO. The CEO/COO presents the project for approval to the JSC/Board. He also reviews the project status, and assists in the remediation of project risks and problems. The CEO/COO is also responsible for managing timely decision making and approvals from the JSC/Board. He usually appoints a Senior Director from operations to be the day-to-day project sponsor who is responsible for stewardship of the project. The CIO is generally responsible for the technical direction and approach, and IT resources to execute the project.

3) Engineering Review Board

An Engineering Review Board (ERB) is comprised of technical strategists and architects from the PSO who are responsible for designing and overseeing the current technical

architecture(s), evaluating future technologies, defining architecture standards and guidelines, managing technology life-cycles, and making recommendations to the PSO Executive Management and Joint Steering Committee/Board regarding technical issues that arise from the project or within the project.

4) Project/Program Management Office

The Project/Program Management Office (PMO) is a PSO body of experts in Project Management (PM) processes and standards. As PM experts, the PMO are responsible for the establishment, dissemination, and training of project management and SDLC methodologies and standards, project manager mentoring, and the assistance in the creation and review of project plans. The PMO may actually house PM experts who are to be deployed to the specific technology project. In some cases, the PMO provides management and reporting oversight of the technology project, particularly in large, multi-release programs.

5) Program Manager and others

The Program Manager (Project Manager for smaller technology implementations) has day to day responsibility for managing the entire collection of releases and projects, and their corresponding budgets, schedules, resources and issues. The PM is usually partnered with an IT Program Manager as well (who ensures IT delivery), and is supported by Release Managers (Project Managers), and various functional managers for Stakeholder Management, Integration, Testing/QA, Training, and Deployment.

b. Reporting, Monitoring, and Issue Resolution Processes

The above bodies all play important roles in Project Control processes that include: overseeing the project, resolving issues, managing risks, and ensuring on-time, within budget, high quality solutions. Each will play a different role, and be given different authorities and responsibilities. To avoid rehashing the fundamentals of Project Management (see Section *VI. Appendix A: PSO IT Best Practices Guidelines)*, only reporting, monitoring, and issue resolution processes will be discussed. These Project Control processes are important disciplined, consistent management activities that aid in the minimization of decision making delays, and will be discussed in that light.

1) Project Reporting and Monitoring

Project Reporting and Monitoring involves the weekly, bi-weekly, monthly and milestone accumulation and communication of project status information, as well as Project Audit activities.

a) Status Reporting

The Program Manager meets with his team and collects and summarizes team leader and member status reports on a weekly basis to update the Project Plan and budget. A weekly program status report is created to communicate the schedule and budget status of the project. This report summarizes work accomplished and planned, the status of deliverables and milestones, and outstanding issues and major project risks. It is sent to the Project Sponsor and PMO.

On a bi-weekly basis, the Program Manager meets with the Project Sponsor to review the project status. Important issues that need escalation to the CXOs and Joint Steering Committee/Board are discussed, with the turnaround time required to avoid schedule and budget slippage. The Sponsor escalates and ensures speedy resolution.

A Project Report Card as described previously should be created on a monthly basis to depict schedule status, budget, staffing status, issues, and watch areas. This dashboard-like report uses either a point system or color codes (red, yellow, green) to indicate relative degree of concern in each area (danger, caution, on-track). Issues and proposed scope changes are detailed out, with schedule and cost impact identified for each. This report is sent to the Sponsor, CXOs, PMO (who accumulates and rolls up all into an overall enterprise-wide status for all work activity), and the JSC/Board.

b) Monthly JSC/Board Meeting

The Program Manager and/or Sponsor presents the Project Report Card to the JSC/Board each month. It is the responsibility of the JSC/Board to stay up to date on the status of the project as well as the risks and issues that are impacting the successful outcome. They should resolve outstanding issues and approve or deny changes of scope (more describing this in following section). By approving any scope changes, they are explicating authorizing either schedule changes and/or budget changes.

Issues that can't be resolved at the meeting should be assigned to a member of the JSC/Board to resolve with a specified timeframe. The JSC/Board should be apprised of the impact to the schedule and budget of any delay in meeting the specified due date.

c) Project Audits

Periodic Project Audits are conducted (see in previous section of report) to evaluate the health of the project from an independent or third party perspective. This monitoring is critical, and often provides a mechanism to emphasize the schedule/budget impact of outstanding decisions that need to be resolved, as well as reinforce a Program Manager's concerns about resource shortages, unrealistic schedules, etc. In this way, the audit should be positively welcomed by the Program Manager and team, versus dreaded as an exercise in criticism.

2) Issue Resolution

The Issue Resolution process is one of the most important Project Control activities performed that will enable successful project completion. Throughout the course of the project, issues that could hinder the ability to meet the schedule and budget are captured in formal Issue Reports. Each report defines the issue, the identifier, category, date identified, person(s) responsible for resolution, priority, due date, and final resolution. It is extremely important that the due date set is both achievable, as well as aware of the potential impact to the schedule.

To manage the list of all issues, an Issue Log is created and tracked. The weekly and monthly status reports should provide a summary of the disposition of these issues. The weekly team status meetings, bi-weekly Sponsor status meetings, and monthly JSC/Board meetings must allot time to review and resolve the issues. Project schedules and budgets should be updated regularly to reflect the impact of any delays as a result of open issues.

It is often necessary to conduct specific, weekly (sometimes daily) issue review meetings to ensure that issues are being resolved in a timely manner, and project delays are avoided. These meetings would include the Program Manager, key Stakeholders and team members, and sometimes the project Sponsor. In some cases, there may be a need to include the JSC/Board if critical, project stopping issues are identified.

As part of the Issue Resolution process, a formal issue escalation process should be defined and followed that would categorize issue types that need to obtain JSC/Board input, review and/or approval.

Issues that have the ability to cause major project delays if not resolved, or significantly impact the overall schedule and budget of the project due to potential scope changes should be given high priority status. In addition, a detailed Impact Analysis should be undertaken, with the results captured in the Issue Report, Log and regular Status Reports. The Impact Analysis should detail the cost and schedule ramifications of the issue (or resolution of the issue) and be communicated early and often to prevent the issue from turning into an after-the-fact Change Notification (discussed in next section).

3. Change Control

A well defined Change Control process administered by the Program Manager and supported by the overall Governance of the project will objectively identify, analyze and report the impact (schedule/costs) of decision making delays and other factors that may impact the cost/schedule/scope of the project.

a. Definitions

1) Change

A Change is anything that occurs on the project that impacts schedule, budget, effort; or depth, breadth, or quality of the deliverables. The baseline upon which to measure against is the Statement of Work or Project Definition contract that was agreed to and signed off on at the onset of the project. The SOW identified the objectives, scope, approach, schedule, budget, deliverables, roles and responsibilities, risks and assumptions, and project management control processes (including change control) of the project. Any changes to those areas will result in a Change Request or Notification.

2) Change Request

A Change Request is a change that requires *approval* by the appropriate authority to implement the change. It is generally a change that will increase the originally defined effort specified in the Statement of Work. The following are common items that require a Change Request:

- Additions to or deletions from the scope items listed in the SOW
- Additions to or deletions from the project activities defined in the SOW
- Additions to or deletions from the deliverables defined in the SOW
- Externally imposed changes to the baseline schedule defined in the SOW
- A change in roles and responsibilities, or reallocation of project staffing
- Any rework of completed activities or accepted deliverables
- Investigative work to determine the impact of major changes* (change request to create change request) – generally if the impact analysis exceeds 4 hours

Change Requests can be originated from within the Project Team, the JSC/Board, external Stakeholders, Regulators, etc. They may arise as the result of the resolution of an issue. They should be documented and logged upon immediate awareness, and follow the agreed

upon Change Control process for authorization. They are not acted upon until written approval is granted.

3) Change Notification

A Notification is a change that requires acknowledgment by the appropriate authority of a change that has occurred that has impacted the schedule and budget of the project. It is generally a change that has delayed or hampered the effort. Proactive identification of these changes before they occur can be a strong project control activity that raises awareness to the JSC/Board of the potential impact to the schedule and cost of the project due to delay. The following are common items that may impact schedule and costs and require a change notification:

- Delays caused by slow issue resolution or Regulatory/Stakeholder decision making
- Assumptions listed in the SOW that do not remain valid
- Delays caused by not having project resources available per the schedule
- Delays caused by missing documentation or lack of access to key subject matter experts
- Delays in the acceptance of deliverables
- Variances of actual work effort from estimated effort
- Changes in the cost of a resource versus the SOW cost

Change Notifications are generally identified by the Program/Project Manager while performing daily, weekly and monthly schedule and budget review, as well as status reporting. They usually arise as the result of the identification of an issue. The above identified items that may hamper the project should be monitored closely, and documented and logged when they have impacted the schedule/budget of the project. The Change Notification should follow the agreed upon Change Control process for acknowledgment. They do not require approval for future action, as they are documenting the past.

Some Notifications that cause project delays can stop the entire project altogether, some will affect only limited work streams, some will cause future rework, and some fall in between. It is important to distinguish the level of magnitude and analyze the schedule and cost impact accordingly.

b. Change Control Process

The Change Control Process should be outlined in the Statement of Work/Project Definition. If not, it should be jointly defined by the Sponsor, Program Manager, and JSC/Board at the onset of the project. It is important to document and communicate the process to ensure that all parties involved in the project understand what constitutes a Change Request or Change Notification, and how it is identified and resolved. In addition, it should be defined who has responsibility for approving them, and the turnaround time required. The Change Control Process should include the following steps:

1) Identify and Record Change/Notification

The Change is assigned a Change number and recorded in a Change Log. Each entry in the Change Log defines the change, the originator, type, priority, date identified, and detailed description.

2) Assign Change for Impact Analysis

The Program Manager administers the Change Log daily, and assigns himself or a member of the project team the Change to perform an Impact Analysis. The Impact Analysis is the critical review of the cost and schedule implications of the Change.

3) Perform Impact Analysis

The Impact Analysis involves the review of the change, and its impact on the scope, deliverables, quality, resources, schedule and costs of the project. Depending upon the type of Change, there may be alternative ways to implement the change. They should be documented and analyzed. The recommended approach to handling the change should be supported by detailed review of the effort by resource to complete the change, as well as the impact to the overall schedule.

4) Complete Change Control Report

The Impact Analysis is documented on a standard Change Control Report. It details the type of change and its impact on the original budget, work effort, and schedule. The Change Control Report identifies the detail work breakdown by resource that must occur to complete the change (or has occurred due to delays). A proposed new Project Plan and Budget is created and attached to the report. The report includes a recommendation regarding the pursuance of the change, or suggestions regarding the mitigation of the impact as a result of a change notification. It should be noted that the Change Control Report serves as an addendum to the SOW/Project Definition document, and is treated as a contractual document itself. Once approved, it is sent to the appropriate Contracts Management or Legal department, as well as Finance, to incorporate any budget changes required.

5) Submit Change Control Report for authorization/acceptance

The Change Control Report is submitted to the appropriate authority for review. This can be as part of the regular status reporting meetings, or as needed. The authorizer may require additional information, defer, or outright reject the Change Request. A Change Notification requires the authorizer to review and understand the impact of project delays, and acknowledge such with his signature. Forward signed document to appropriate Contract, Legal and Finance departments.

6) Update Project Plan, Budget, and Change Log

Upon acceptance of the Change Control Report, the Project Plan and Budget are updated to reflect the impact of the Notification, or the addition of new activities, tasks, resources, and deliverables. The Change Log is updated with the resolution.

7) Implement Change Request

The Change Request incorporated into the new Project Plan is implemented as any other project task. It is tracked separately within the overall plan for ease of schedule and budget maintenance, as often the Change Request is allocated different charge codes.

8) Manage Change Log

The Program Manager must manage the Control Log on a daily basis to ensure that all changes to the project are identified, assigned, analyzed and resolved in a timely manner.

c. Figure 25 – Example Change Control Report Page 1 of 2

SECTION 1

Change Type:	**Request ☐ OR Notification ☒**	**Change #:**	**1**
Change Description:	**<Enter short change request description for title>**		
Originator:	<Enter name who identified change>	**Date Originated:**	1/1/04
Assigned to:	Project Manager	**Priority:**	High

Change Request/Change Notification Information

Request:	**Notification:**
☐ Addition/Deletion of Scope	☐ Change in Assumptions
☐ Addition/Deletion of Project Activities	☐ Resources not available according to schedule
☐ Addition/Deletion of Deliverables	☐ Access to information/resources causing schedule slippage
☐ Change in staff responsibilities	☐ Delay in decision making/acceptance of deliverables
☐ Rework of completed activities/accepted deliverables	☐ Work effort variance
☐ Other:	☐ Change in resource cost
	☐ Other:
☐ Investigative work to determine impact of major changes	

Detailed Description of Change Request / Change Notification:
<Enter detailed description of change request or notification. Explain the cause or need for change. Identify potential schedule, resource, and cost impacts that need to be further analyzed>

Budget Impact		**Effort Impact**		**Schedule Impact**	
Original/Prev Total Budgeted $:	$1	Original/Prev Total Hours:	1	Original/Prev Project Start:	1/1/04
Revised Total Budgeted $:	**$1**	**Revised Total Hours:**	**1**	**Revised/New Project Start:**	**1/1/04**
Change $ Estimate:	**$1**	**Change Hour Estimate:**	**1**	Original/Prev Project End:	1/1/04
				Revised/New Project End:	**1/1/04**

d. Figure 26 – Example Change Control Report Page 2 of 2

SECTION 2

Change Type:	**Request or Notification**	**Change #:**	**#**
Change Description:	**<enter short change request description>**		

Breakdown Analysis of Change

Estimates	Business Analysis	Project Mgmt.	Design	Coding / Testing	Documentation	Other	Total
Effort Hour Estimate							
Resource Allocation (Role - Hours)							
Cost Estimate (Role Hours * $/Hr)							

Recommendations and Review

$/Schedule Analysis Comments: (Summary and analysis of impact on current schedule)
<Enter explanation of the impact of change on schedule and budget>

Originator's Recommendation:
<Based on detailed schedule and budget analysis, original identifier of change enters recommendation of action>

Approval/Acknowledgment of Change Request/Change Notification

Approved By:	<Approved by Name>	_____	**Date:**	1/1/04
Resolution Status:	Assigned	[Approved, Rejected (CR), or Deferred (CR)]		

Reason for Rejection/Deferment: (Change Request only)
<Enter explanation for a rejection or deferment of a change request>

Attachments: (1) Project Plan (2) Budget Analysis

I. What Cyber Security issues should be considered during the applications acquisition and development process?

The typical SCADA system in the past was designed to be extremely reliable and highly available, operating 24 by 7 by 365, with almost no downtime for maintenance. Security was provided by keeping the SCADA network physically separate from other networks and, in many instances, a firewall was used as a divider between the SCADA network and the corporate network. Due to this history, cyber security for SCADA is an area which has not received a lot of attention.

In recent years, because of Internet drivers and regulatory needs, SCADA systems have been forced to be more open. The impact of wholesale competition has resulted in the need to connect to new information systems necessary to facilitate the marketplace functions. Proprietary protocols have been replaced with IP-based protocols such as ICCP and DNP3 for communicating electric system data between utilities, RTOs, ISOs, etc. This has resulted in less expensive systems but a much increased level of vulnerability.

In addition, as systems have become more open, support for SCADA systems has become more fragmented. Systems can be supported by the SCADA Operations Group, the IT Support Group and Security Group, each with separate budgets and objectives. The following recommendations are made to address this area:

1. Understand and comply with NERC security Standards
   - NERCs Standard 1200 adopted August 2003 and extended through August 13, 2005 to "reduce risks to the reliability of the bulk electric systems from any compromise of critical cyber assets"
   - Mandatory compliance with Standard 1200 by 1Q2005 is required for those entities under FERC oversight
   - The anticipated permanent NERC CIP-002-1 through CIP-009-1 will have fines and penalties for non-compliance
2. Assess overall cyber security risk recognizing that the NERC standards are minimum requirements.
   - Identify all connections to external networks
   - Identify use of dial-in modems by support personnel, vendors, etc.
   - Determine password policies and usage
   - Identify methods used for remote access
   - Identify how RTUs are connected to EMS systems
   - Identify protocols utilized & encryption if any
3. Determine the hardware and software security requirements and design security features at the beginning of the project to ensure that cyber security is integrated throughout the entire system and not treated as after-thoughts.
4. Use firewall only as a first step to protect the SCADA network. It alone does not provide adequate protection between SCADA and corporate networks and will not prevent application-level attacks or virus impact.

5. Use gateway protection which combines firewall, intrusion detection and anti-virus functions.
6. Use a VPN (Virtual Private Network) for secure communications between remote users and the operations networks.
7. Use intrusion detection which is protocol anomaly-based as well as signature-based.
8. Ensure compliance with password policies.
9. Use anti-virus on all systems connecting to the operations networks.
10. Establish effective patch management procedures.
11. Establish effective incident response and recovery plans.
12. Disable unused network services and ports.
13. Disable unauthorized, invalid, expired or unused computer accounts and physical access rights.
14. Use effective password management that periodically requires changing of passwords, including defaults.
15. Secure dial-up modem connections.
16. Install and update anti-virus software.

VII. Appendix A: PSO IT Best Practices Guidelines

A. Section Summary:

Recommendations for managing IT organizations in a regulated, cost minimization environment are presented in this section.

Power System Operations organizations require very complex technical environments and fairly large technical organizations to perform the engineering analyses and process the transactions necessary to manage reliability and administer the markets. It is critical that the IT organizations be focused on achieving operational excellence and have instilled a mindset of continuous improvement. However, because of the regulatory environment in which the PSOs operate, the IT organizations need to be fiscally prudent in their pursuit of operational excellence. The implementation of technical Best Practices, therefore, needs to be implemented within the context of cost minimization. As the responsibility of the PSO is expanded, additional expenditures may be warranted as the criticality of its operations increases. However, many Best Practices do not require large expenditures of funds but are, rather, dependent on, and a function of, a disciplined, process centered organization.

Best Practices for the following areas are detailed in this section:

A. IT Organization and Culture

B. IT Governance

C. IT Strategic Planning and portfolio Management

D. Vendor Evaluation / Vendor Management

E. Data Center Operations

F. Back-up & Restore

G. Network Operations & Management

H. SCADA Support

I. Capacity Planning & Performance Management

J. Project Management and SDLC Methodology

K. Engineering Review Board

L. Problem Resolution Management

M. Root Cause Analysis

B. Introduction

The PSOs require very complex technical environments and fairly large technical organizations to perform the engineering analyses and process the transactions necessary to manage reliability and administer the markets. It is critical that the IT organizations be focused on achieving operational excellence and have instilled a mindset of continuous improvement. However, because of the regulatory environment in which the PSOs operate, the IT organizations need to be fiscally prudent in their pursuit of operational excellence. The implementation of technical Best Practices, therefore, needs to be implemented within the context of cost minimization. As

the responsibility of the PSO is expanded, additional expenditures may be warranted as the criticality of its operations increases. However, many Best Practices do not require large expenditures of funds but are, rather, dependent on, and a function of, a disciplined, process centered organization. The following sections detail many of the Best Practices that Gestalt believes should be implemented at the PSOs.

C. IT Organization and Culture

1. Culture

Gestalt has found that highly effective, mature IT organizations have the following characteristics:

a) Clear and articulated organizational purpose, strategy and business alignment

b) Integrated, routine, flexible planning process

c) Committed, effective leadership and technical governance

d) Skilled, experienced, trained, productive employees

e) Clear organizational and individual roles, responsibility, and accountability

f) Well defined, documented, and communicated policies, processes and procedures

g) Project management discipline

h) Operation and service orientation

i) Architectural aligned investment strategy

a. Clear and articulated organizational purpose, strategy and business alignment

IT organizations that are closely aligned with the business have clear executive agreement on the role and purpose of IT within the organization. Executive agreement on the role of IT involves an understanding of business and technological objectives, expectations, and capabilities, and a determination of where IT fits from an enterprise-level perspective regarding strategy, investment and operations. Organizations should decide whether they view IT as a revenue generator/profit center by offering IT products and services to the market, as a leading strategic asset essential to driving growth, as a partner in achieving business operational objectives, or as a service provider focused on cost and performance. While many IT organizations would like to be a profit center or a strategic asset, most are relegated either to a partner or service provider. Organizational capabilities often drive the perceived role of IT and should be considered as either constraints/opportunities when defining IT's purpose and role; they should not, however be key determinants.

The IT organization should have a clearly defined, documented, and communicated strategy that reflects a clear understanding and agreement between business and IT executives regarding the IT organization's role. It is essential to develop and align the IT strategy in conjunction with the overall business strategy. For instance, if the business strategy is punctuated with operational efficiency goals, the IT strategy should be reflective of cost containment or cost reduction goals as well; under this scenario it would be inappropriate to have IT goals focused on IT becoming a competitive differentiator or product innovator. The IT Strategy should include long term

objectives for the IT organization, short term goals, measures, and key initiatives to be undertaken to achieve these goals.

b. Integrated, Routine, Flexible Planning Process

Like strategy, it is essential to integrate business and IT planning such that the IT plans are driven by business needs. The IT Plan should ensure that the organization is "doing the right things" to meet business objectives. The IT organization should have a well defined, and adhered to, annual planning and budgeting process and the IT plan should be clearly communicated to the rest of the organization. The IT plan should serve as a "roadmap" to guide the activity of the IT organization through the next three years, with specific detail and emphasis on the one year horizon. The initiatives and projects defined in the plan should be described in enough detail to determine overall costs, benefits, resource requirements, approach and timelines. Critical dependencies between projects should be analyzed, and overall timing and investment should be driven by business priorities. The plan should not become "shelfware", but should be regularly reviewed (i.e. quarterly) for performance and adjusted when circumstances arise and priorities change. The plan should have clearly defined metrics to against which performance is measured.

c. Committed, Effective Leadership and Governance

IT Leadership (CIO/CTO, Directors, VPs, etc.) should be experienced in both the IT and utility industries, and have a high degree of business and technical knowledge. They should understand the PSO business and work closely with the business leadership to define and communicate IT's role within the organization. The IT leaders should be focused on setting the strategic IT direction, planning, resource management, and oversight of operations and initiatives. They should demonstrate strong relationship management skills with their business peers, and strike the right balance between strategic and tactical priorities.

Organizations that seek to have the greatest level of business and IT alignment position the CIO/CTO equally with the other CXOs, demonstrating that IT is a valued partner and equal contributor in the execution of the business's strategy.

d. Skilled, Experienced, Trained and Productive Employees

The IT personnel should be technically adept and have sufficient experience within the IT and utility industry. While many PSOs rely upon external contractors for applications and infrastructure development, they should hire and develop the appropriate number of skilled and experienced employees to maintain and operate the systems and technologies that are being developed and installed. A multi-year staffing plan and employee development plan should be constructed based upon the results of the IT planning process. IT personnel should have strong vendor management skills in this environment, as well as good business relationship capabilities. In organizations where outsourcing has been chosen as a resourcing strategy, IT personnel should have strong architecture, project management and methodology skills.

There is a growing trend within mature IT organizations to add business savvy, financially skilled resources to their organizations to move towards a "run IT like a business" (RITLAB) model. These resources assist in the strategy, planning, and financial analysis of project portfolio management.

Because IT skill requirements are often poorly understood outside of the IT organization, many IT organizations are adding Human Resource managers and/or analysts to their department to

perform staff planning, hiring, orientation, competency / skills inventory, communications, performance planning and evaluation, and training (instead of using the corporate HR function). Regardless of where this function is located organizationally, the processes described should be performed to attract, retain, and grow skilled, experienced and productive employees.

A balance of skills, capabilities, and personal styles is required to fulfill the variety of IT roles and responsibilities. An imbalance in styles and approaches will limit the effectiveness of the organization. When technical knowledge overshadows business knowledge, organizations typically develop technology for technology's sake and not to meet business needs. On the other hand, when technical knowledge is lagging, solutions are often ineffective, long in development, and quickly outdated.

e. Clear Organizational and Individual Roles, Responsibility, and Accountability

There should be a well circulated document that states the purpose of IT, the organization structure, the charter of critical functions of the IT organization, and the roles and responsibilities of the personnel within each of the groups. Additionally, the business community should understand and be in agreement with these roles and responsibilities. Each individual should have clearly defined and documented role expectations and regular (semi-annual) performance appraisals.

f. Well Defined, Documented, and Communicated Policies, Processes and Procedures

Mature business and IT organizations provide responsive, consistent, and efficient service through the seemingly effortless execution of a standard set of operational policies, processes, and procedures. These policies, processes, and procedures are well documented, distributed, updated, consistently applied, and effectively managed.

Policies establish the overall rules of engagement and guidelines for managing the business. Policies typically cover technology usage, purchasing practices, hiring, compensation, separation practices, financial reporting and budgeting practices, and other administrative functions. Well documented and communicated policies provide a means of ensuring that common management functions can be executed consistently throughout an organization.

Processes typically describe the work flow associated with managing a set of interrelated activities. Typical processes would include change management, release management, project management, problem management, and client relationship management. Processes typically have owners who are responsible for periodically documenting, distributing, and updating the processes, as well as ensuring that the processes are working effectively at all times.

Procedures describe the steps required to perform a specific task. Procedures are typically operational in nature and provide the instruction which ensure that the task will be carried out safely, efficiently, and consistently. Common procedures, for example, would include back-up and restore procedures for servers and databases, re-boot instructions, or installation of equipment.

g. Project Management Discipline

The credibility and trust in an IT organization relies upon its ability to deliver the agreed upon scope on time, on budget with a high degree of user satisfaction. Cost, scope, and schedule management along with adherence to common standards and methodologies are key components of project management and should be essential elements of any organization that routinely

manages large and small projects. Mature organizations have a well documented, disseminated, and adhered to project management methodology. Not only are IT Project Managers trained in the methodology and techniques of project management, but all individuals are given overviews and/or training as well. Many organizations require their PMs to receive board certification (i.e. Project Management Institute). In addition, those organizations with a strong project management discipline usually establish a Project/Program Management Office (PMO) to provide a central repository of knowledge and resources to perpetuate the practice. These organizations are able to better utilize their resources, accurately plan and deliver within their budgets and schedules, and create better user satisfaction.

h. Operation and Service Orientation

Mature IT organizations provide consistent, uninterrupted service and support to the business. While ensuring that the "lights stay on" is often not glamorous, it is a key determinant in obtaining and maintaining the trust and respect of the business community. Those organizations that provide a high level of operational reliability are better aligned with the business, and usually treated as partners in strategic decisions. The business community is more likely to seek assistance from the internal IT organization then go to outside contractors when looking for IT solutions if they believe that the internal IT organization has the skills, discipline and focus to deliver.

IT organizations that have a strong service orientation break down the "us vs. them" mentality that often exists between IT and the business. They generally are structured to have a customer facing function or organization that has the responsibility for managing internal customer relationships. If they don't have this function or structure, the applications group managers who are responsible for managing applications on a line of business basis should also be responsible for managing the overall IT / client relationship. Their internal clients should always know who they are supposed to contact for specific service requests and problem types.

Performance measurements for applications, infrastructure, and IT service offerings should be defined jointly with the internal client groups. These performance measures should be tracked constantly, and reported and reviewed on a routine basis (daily, weekly, monthly, quarterly, semi-annually, annually) depending upon the type and importance.

Internal Service Level Agreements (SLAs) based upon these performance measures should also be jointly defined with the internal client groups and business executives. The SLAs represent the agreed upon performance target for each defined area. In the absence of verifiable performance data and agreed upon service levels, clients rely on single data points or recent events to drive their perception of service. In addition, client expectations for system availability and performance may often be much higher than the IT organization's expectations and resource capabilities and availability (technical and human).

The SLA's should minimally address system availability, on-line response time, job execution times, problem resolution durations, maintenance windows, project related items, network performance, turn around time on new equipment orders, security access, and system modification requests, and communications with the user community.

i. Architectural Aligned Investment Strategy

Mature IT organizations define and implement a forward looking architecture strategy to guide the organization's decision making regarding future technology investments. The architecture

strategy entails all areas of technology assets: infrastructure, application, data, communications, security, facilities, processes, and people. It defines the products, configuration, guidelines, standards, and future direction of each of those areas. It identifies and evaluates the feasibility of emerging technologies, and makes recommendations regarding their maturity and fit. When new business requirements arise that seek technology solutions, the architecture strategy is a key criteria in evaluating, prioritizing, and approving new projects. Organizations without a robust architectural strategy create a large, expensive, heterogeneous technical environment that constantly consumes limited IT resources (budget, human), is difficult to maintain and does not allow for cost effective integration of data and processes. Many mature organizations have created an Architectural Review Board that operates in parallel with a Joint Steering Committee in evaluating and prioritizing projects.

2. Governance

Governance is the process of setting direction and providing oversight to ensure that the direction is achieved. In addition to being a service provider, the IT organization must also function as the steward of the organization's technology assets. It must, therefore, establish the necessary controls to safeguard the organization. Below are some governance bodies and roles that provide direction and oversight to the strategy, planning, resource management, and execution of IT operations and initiatives.

a. Joint Steering Committee

A Joint Steering Committee (JSC) consisting of formal board of business and IT executives (CXOs), Business Unit and IT Directors, and Corporate Strategy, Finance and Planning Managers should be established to provide the governance and oversight for enterprise-wide IT planning, budgeting, prioritization, and disposition of technology initiatives. The JSC should work in conjunction with the overall corporate strategic planning and budgeting processes.

The Joint Steering Committee should have a defined schedule of meetings and an established planning horizon. Ideally the JSC would execute a major direction-setting strategy/planning process annually, major reviews for adjustments quarterly, and status reporting that also considers urgent needs/requests on a monthly basis. The JSC must establish the following procedures and controls to perform their function: agreed upon manner of decision making (consensus, weighted voting, single decision maker, etc), standard format for submitting candidate initiative/investment requests (business case, project definition, etc.), thresholds to control the number of initiatives/investments under consideration (financial, resource, physical number, etc.), and an objective set of criteria linked to the business strategy and objectives that will be used to prioritize decision making.

b. IT Executive Management (CIO, CTO)

Overall IT management is lead by a Chief Information Officer (and/or Chief Technology Officer). To achieve greatest alignment between IT and the business, it is recommended that the CIO be positioned equally with the other CXO positions in the organization.

The CIO performs four major functions: (1) builds internal and external partnerships to meet shared enterprise objectives and strategy, (2) builds and manages a capable IT organization, (3) designs and manages mature processes (technical, administrative, procurement, and business), and (4) delivers technological services and products.

c. Engineering Review Board

Many organizations have created an Architectural Review Board that operates in parallel with a Joint Steering Committee in evaluating and prioritizing projects using a technology investment-focused lens. The Engineering Review Board (ERB) is responsible for designing and overseeing the current architecture(s), evaluating future technologies, defining architecture standards and guidelines, managing technology life-cycles, and making recommendations to the Joint Steering Committee regarding proposed initiatives that impact the current/proposed architecture.

d. IT Project/Program Management Office

The IT Project/Program Management Office (IT PMO) should be established to be a custodian of the Project Portfolio of IT initiatives and an internal body of experts in Project Management (PM) processes and standards. Many organizations have historically established an IT PMO primarily for the latter reason, but are beginning to embrace Project Portfolio Management and see this as the construct to support it. *See Appendix A: PSO IT Best Practices Guidelines for additional discussion regarding the ERB.*

As custodian, the IT PMO should provide an overall view of all projects and work to resolve conflicts that exist between projects. They would be responsible for: the maintenance of the IT Project Portfolio (Portfolio) as new investment/initiative requests arise and business priorities change, the allocation and optimization of IT resources to support the Portfolio, the execution of project audits, and monthly status reporting of all initiatives. They would support the Joint Steering Committee in making prioritization decisions.

As experts in Project Management, the IT PMO would be responsible for the establishment, dissemination, and training of project management and Systems Development Life Cycle (SDLC) methodologies and standards, project manager mentoring, assistance in the creation and review of project plans. They would also maintain the IS organization's repository of reusable project-related artifacts (e.g., project plan templates, estimating models, and components), best practices, lessons learned, and recommended tools selection and usage. The IT PMO may actually house PM experts who are to be deployed to specific IT projects.

The size of the staff and the skills embedded within the IT PMO office vary depending on the role that it is designed to play. In the PM Experts role only, the IT PMO requires a Program Manager to oversee it (who will double as an best practice expert if the total IT PMO size is under five FTEs), relationship managers to develop requirements with the business, methodology experts, project managers, and a project librarian. The IT organization will need to determine whether all project managers will organizationally reside within the IT PMO or whether some PMs will be located in other IT or business organizations. Organizations with an established IT PMO will often house a very small number of experienced project managers who have responsibility for enterprise-wide projects. Smaller projects are then managed by personnel located in other organizations but use the standards set forth by the IT PMO.

In the more complex model where the IT PMO acts as custodian of the IT Project Portfolio (in addition to PM Expert's role), the staffing size and mix will change. The stature of the IT PMO leadership would need to be elevated to a Director or higher level within the organization. Master planners, additional best practice experts (financial, staffing), additional project managers, and administrative staff need to be added.

Typical staff roles and activities performed are depicted in the next Figure:

e. Figure 27 – PMO Roles and Responsibilities

Role	Activities Performed
IT PMO Director/Program Manager	IT PMO Management and Oversight
Master Planners	Project Portfolio Updates and "what-if" analyses
	Resource Allocation/Optimization
	Joint Steering Committee support (monthly status)
	Scheduling
Project Managers	Project specification and planning
	Project Management for enterprise projects
	Project Mentoring
	Project Audits
Relationship Managers	Business interface
	Development of project requirements
	SLA development and administration
	Budget or chargeback support
Best Practice or Process Experts	Training
	Project mentoring
	Quality assurance
	Methodology and Standards development
	Financial analysis of candidate initiatives/investments
Librarian	Project records
	Standards
	Project repository maintenance
Administrative support	Back-office support
	Reports

3. IT Organization Functions/Processes

The Chart below maps the IT Processes to the IT Organization Functional Areas that are either Owners or Participants of the process. The structure of the IT Organization may change across PSOs, but the general functional areas and processes should be similar. Hence, the corresponding Owner of a process would likely change under different structures. The IT Functional Areas depicted below presume the following: an active Project Management Office function that leads planning and portfolio management, a Strategy and Architecture Group that leads IT strategy and architecture management, and Business Area Relationship Managers who manage the interaction between the clients and supporting Business Applications.

a. Figure 28 – IT Processes / IT Organization Matrix

RTO/ISO - IT Processes/IT Organization

Process Area	CIO/CTO	Project Mgmt Office	Management Staff	Strategy & Architecture	Management & Staff	Business Applications	Management & Staff	Market Applications	Settlements & Accounting	Corporate Applications	Transmission Applications	Infrastructure	Management & Staff	IT Communications	Data Management	Systems Administration	Desktop Administration	Security Administration	Access Mgt & Help Desk
Perform Account Management																			
Understand Customer Requirements			P		P		O	O	O	O	O		P	P	P	P	P	P	P
Administer SLA's and Track Performance							O	P	P	P	P		O	P	P	P	P	P	P
Manage Customer Relationships							O	O	O	O	O		O	P	P	P	P	P	P
Administer Management Controls																			
Establish IT Management Controls			O		P		P						P						
Establish IT Policies & Procedures			O		O		O	P	P	P	P		O	P	P	P	P	P	P
Establish Change Management Controls			P		O		P						P						
Establish Project Management Controls			O		P		P						P						
Establish Security Controls					O		P						P						
Perform IT Planning & Administration																			
Conduct Research					O		P						P						
Define IT Strategy & Plan			O		P		P						P						
Develop IT Architecture					O		P						P						
Establish IT Standards			P		O		P						P						
Manage IT Budget			O		P		P						P						
Perform IT Supply Chain			O		P		P						P						
Perform Vendor Management			O		O		O						O						
Manage IT Human Resources			O		O		O						O						
Implement Solutions																			
Determine Solution Requirements			P		P		O	P	P	P	P		P	P	P	P	P	P	P
Plan & Design Solution			P		P		O	P	P	P	P		P	P	P	P	P	P	P
Build Solution			P		P		O	P	P	P	P		P	P	P	P	P	P	P
Test Solution			P		P		O	P	P	P	P		P	P	P	P	P	P	P
Deploy Solution			P				O	P	P	P	P		O	P	P	P	P	P	P
Maintain Solution							O	O	O	O	O		O	O	O	O	O	O	O
Provide Operational Support																			
Perform Operations													O	O	O	O	O	O	O
Manage Configuration					P		P	P	P	P	P		O	O	O	O	O	O	O
Manage Facilities														P		P			
Perform Problem Management			P		P		P	P	P	P	P		P	P	P	P	P	P	O
Perform Change Management			P		P		P	P	P	P	P		P	P	P	P	P	P	P
Perform Capacity Planning			P		P		P						O	O	O	O			
Provide Backup Capability					P										O				
Perform Disaster Recovery					P		P						O	P	P	P	P	P	P
Perform Asset Management			O		P		P						O						

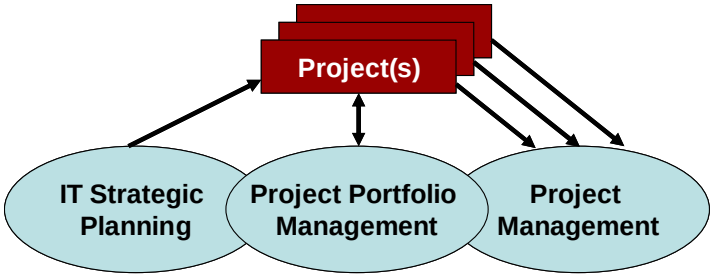
Key: O Process Owner
P Participant

Note: the CIO is the ultimate Process Owner and Participant for all processes but where no other owner is defined, will be depicted as Process Owner

D. IT Strategic Planning and Portfolio Management

There are several levels of IT strategic planning and management functions that should be in place to guide the efforts of the IT organization. At the macro level, an annual integrated business and IT Strategic Planning process should be instituted to guide the intermediate and long term direction and strategy for all IT investments and initiatives. Enterprise-wide Project Portfolio Management should be used to manage the synchronization of these interdependent IT initiatives/investments to ensure that the efficient use of resources across multiple assignments are optimized to meet the objectives that are outlined in the IT Plan. At the micro level, formal Project Management methodologies and standards should be employed to ensure the successful execution of each individual initiative or project (*see separate section on Project Management*).

a. Figure 29 – IT Strategic Planning Diagram



2. Integrated business and IT Strategic Planning

Integrated business and IT planning with the proper inputs and rigor ensures that IT remains aligned with business requirements, that IT resources are allocated to the highest priority projects, and that sufficient human and systems resources are available when needed. In the absence of a rigorous planning process, requirements may be missed, resources may not be optimized, and performance may suffer. Without requirements and performance based input, forecasts are not accurate, budgeting becomes impossible, and just-in-time development is required. Solutions are often "quick fixed" to accommodate for shortfalls, or over built to provide unnecessary contingency capacity.

E. Key aspects of IT Planning:

- Integrated with the Business Planning cycle
- Formal, repeatable process
- Guided by joint Business and IT Steering Committee
- Driven by business objectives, goals and initiatives
- Includes a three year Road Map, one year plan with budget and resource requirements, and a definition of near term projects

The organization should adopt and implement an integrated IT and business planning model and use the model to drive the development and expansion of systems, prioritize projects, and set budgets. Inputs to the process should include business strategy, goals and requirements, systems performance, service level data, configuration and resource availability data, asset inventories, and existing resource levels. Business process owners and IT managers should engage in interactive planning sessions to select and prioritize programs and projects, key milestones, and performance metrics. Often a Joint Steering Committee of business and IT executives is created to provide guidance and oversight to the planning process.

The outputs of the integrated business and IT planning process should include three year technology and staffing resource plans, a one year budget, a two year spending forecast, and IT departmental and group level goals and objectives. Gaps between existing and forecasted requirements should be analyzed, and alternative action plans for closing the gaps should be developed. The plan should be updated annually and adjusted as performance or business requirements dictate.

1. Enterprise-wide Project Portfolio Management

In order to ensure the synchronization of interdependent project initiatives and efficiently manage resources across multiple assignments, enterprise-wide Project Portfolio Management (PPM) needs to occur. PPM provides a link between the information and processes used to support IT strategic planning and the project management techniques and processes that govern project execution. It is the continuous process of selecting and managing the optimum set of project-oriented initiatives that enable an organization to deliver the most value and meet the organization's strategic objectives and goals.

F. Key aspects of Project Portfolio Management:

- Guided by joint Business and IT Steering Committee
- Linked to business objectives, goals and budget with clear prioritization categories and weights defined
- Administered by formal structure such as a Project/Program Management Office (PMO)
- Continual portfolio re-alignment
- Manages the weekly and monthly project status reporting in a consistent manner and presentation
- Supported by a well defined set of processes and rigorous tools to support prioritization, resource allocation, reporting and scenario analysis

If the IT Strategy and Plan has created the initial "portfolio" of projects, resource requirements and plans that are linked to the Business Strategy, Project Portfolio Management processes should be followed to monitor the execution of projects, rebalance the portfolio when new requirements arise or business changes occur. The PPM processes should be followed to manage the weekly, monthly, and on-demand status reporting and produce a "dashboard" view of the project(s) health.

A Project Portfolio Management process is most likely to be institutionalized if a joint IT and Business Steering Committee is in place and actively supports the process. In addition, organization resources are required to administer the Project Portfolio. The best solution is the establishment (by the Board) of a Project/Program Management Office (PMO) who has specific responsibility for its custodianship.

If the IT Strategy does not detail the projects that will be undertaken, the Enterprise-wide Project Portfolio Management process can help. The PPM process would start with the identification of all IT related projects (application and infrastructure) across the enterprise, categorizing each project, identifying costs, benefits, and milestones, and linking the resources required to execute the project ("demand"). The inventory is most helpful if all projects can be identified, even those being performed by non-internal IT resources that are located in different lines of business. In addition, all IT resources are also inventoried by skill set to identify the available "supply" of appropriately skilled IT staff and contractors.

After the IT projects are inventoried, each project should be linked back to the Business Strategy and objectives, to show a clear alignment between the efforts of IT and the business community. Analysis of the "portfolio" of projects should occur. This includes evaluating value, risk, project health, resource leveling, IT investment category, etc. Decisions will need to be made regarding

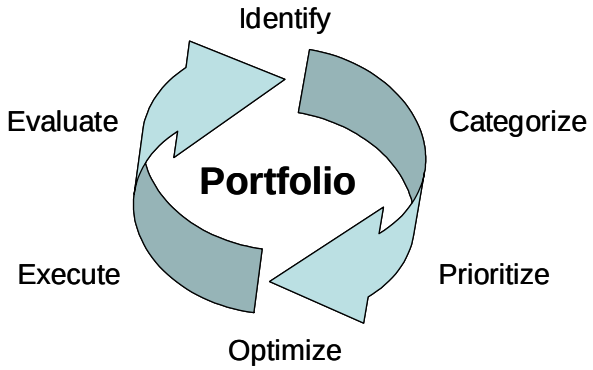
the future status of each project – continue, stop, combine, change scope, change resources or timing of milestones. These decisions should be based upon a formal set of prioritization categories established by the Business and IT Steering Committee. The appropriate mix of project types (strategic, enhancement, utility, etc) should be targeted.

With a targeted portfolio of projects identified, "what-if" analysis should be performed to determine the overall timing and resource requirements of the portfolio. The initial ideal portfolio will be adjusted to take into consideration these and other constraints, with some projects dropping of the list, and others being bumped up. This is an iterative process, and will take several reviews to arrive at the "optimal" mix of projects.

At the completion of the optimization of the portfolio, execution of the projects ensues. During the execution of the projects, detailed project health related information should be reported on a weekly basis and consolidated into an overall executive dashboard (red, yellow, green indicators for different aspects such as budget, schedule, resources, and issues).

The portfolio should be reevaluated on a periodic basis (monthly/quarterly) as new requirements and/or business strategy changes occur. These requests or changes should be analyzed and prioritized against the existing portfolio with adjustments made as necessary. Resources may need to be reallocated or obtained from external sources, and some on-going projects may need to be altered or stopped.

a. Figure 30 – Project Portfolio Management Process



G. Vendor Evaluation / Vendor Management

The PSOs are generally in need of a significant amount of assistance from external vendors for software products, software development and operational assistance. It is critical that the PSOs develop, implement and use rigorous vendor/contract management processes. They should include a standard structured process for the evaluation of vendors that consider all aspects (e.g. cost, terms, previous experience, risk sharing) of solution delivery. There should be provisions for ensuring that Statements of Work are precisely developed and monitored once the engagement commences. Software product and development vendors should not begin software construction until the software designs have been created. A common method of evaluating operational vendors should be developed and the vendors should be rated on a monthly basis.

H. Data Center Operations

Data Center Operations consists of the physical and facility requirements, the network components, mainframe and server operations, storage support, and technical environmental support of the applications that reside on these servers and mainframes. It is important to understand that care and feeding of these Data Centers is of utmost importance to the success of the company. This means, for example, that dual electrical feeds, conditioning/climate control, UPS planning and redundant designs in both server and networking, are all "best practice" data center design practices. The following sections enumerate best practices in several areas related to Data Center Operations.

1. Facility and Physical Requirements as related to Utility and SCADA environments

a) Multiple physically separate connections to public power grid substations (separate substation feeds).

b) Continuous power supply with backup uninterruptible power (UPS) systems.

c) Adequate UPS capacity, air conditioning and proper lighting.

d) UPS testing plan in place and executed according to plan/schedule.

e) Conform to or exceed applicable local structural building codes utilizing standards such as bullet proof glass, fire doors and reinforced walls and complying with disaster proof design.

f) Comply with all local zoning ordinances and requirements.

g) Location certified to not be included in a 100-year flood plain.

h) Earthquake and hurricane bracing on all racks and cable trays (where appropriate).

i) Adequate conditioning, including a backup system for the multi-zone air conditioning.

j) Climate control including humidity sensors.

k) Heat and smoke detectors that meet or exceed all local fire code regulations (OSHA).

l) Very Early Smoke Detection Alarm (VESDA).

m) FM200 [ETG5] or equivalent fire suppression system in data center and NOC.

n) Separate detection/FM200 zone under raised floors.

o) Pre-action dry pipe system zoned to release water only where needed.

p) Easily removable access panels in raised flooring.

q) Flood sensors and monitoring under raised floors and in other critical areas.

r) Grounding plan developed and separate grounding systems designs to prevent grounding loops.

s) Remote monitoring as required for sensitive areas.

t) Formalized physical facility preventive maintenance program.

u) Sub-breakers per relay rack or lineup.

v) Power Plan reflecting state of the art needs.

w) Power filtering in UPS system.

x) Provide access to limited and managed security policies for all facility entrances.

2. Data Center Networking

a) High-end routers (such as Cisco 7500 or 12000 Series) should be arranged in a redundant configuration.

b) Switching and links entirely redundant with no single points or paths of failure.

c) Intrusion detection implemented.

d) All cabling designed to Category 6 specifications (to support 1-Gbps data rates).

e) Communications cabling raceways that are separate (i.e. no intersections) from electrical.

3. Advanced Server Features

a) Virtualization for servers and storage may become a key technology for data centers as a means of improving customer satisfaction levels, promoting higher efficiencies and lowering overhead costs.

b) Server Virtualization allows the de-coupling of logical servers (e.g. messaging, database and domain controllers) from hardware. It also isolates applications from the operating system and aggregates multiple storage resources as one volume.

c) An application-specific environment runs in a protected memory space rather than on the operating system. As Logical servers are converted to virtual servers; they become files not tied to specific hardware, but reside on logical unit numbers carved out of a Storage Area Network (SAN). They can be operated on any physical server or moved to other physical servers without interruption to the users.

d) Efficiencies are derived from the consolidation of processing resources, managing load capacities across a pool of disparate resources and the ability to quickly spin up any kind of server which may be required.

e) The Gartner Group predicts that by the end of 2005, 25% of the Fortune 1000 will use partitioning - a key virtualization technology - for their Windows server deployments. And by 2008, the firm estimates that companies that don't leverage virtualization technologies will spend 25% more for their Intel servers and 15% more for RISC servers, including hardware, software, labor and space.

4. Enterprise Grids

Enterprise Grids consist of large configurations of low cost, clusters of commodity servers intended to significantly reduce the cost of computer hardware. Data Centers, as Enterprise Grids, will have the ability to dynamically change their configuration to meet the changing demands of the business at any moment in time. Application workloads will be managed as services that must meet defined levels of quality. Processing and storage resources will be allocated to services in a fluid fashion to ensure that quality levels are maintained.

Grid computing pools utilize processing cycles from multiple computers to maximize capacity, memory, power and other resources that are distributed across multiple systems. The concept of a grid describes a framework in which heterogeneous and distributed computational, networking,

memory and storage resources can be linked to serve the needs of particular user applications. According to Insight Research, total worldwide grid spending will increase from $250 million in 2003 to approximately $4.9 billion in 2008. The PSOs should continually evaluate the potential use of enterprise grids to satisfy their application's needs.

5. Oracle RAC (Real Application Cluster)

Oracle Real Application Cluster enables the Oracle Database to run mainstream business applications of all kinds (e.g. SAP, PeopleSoft, in-house developed applications, etc.) on clustered database servers. Oracle RAC running on a cluster can provide a very high level of capability in terms of availability, scalability and low-cost computing. If a node in the cluster fails, Oracle continues running on the remaining nodes. If additional processing power is needed, new nodes can be easily added to the cluster. A key feature of this technology is that all data on disk is accessible by all nodes in the cluster; data does not need to be partitioned among the nodes. Dynamic provisioning of nodes, storage, CPUs and memory promote efficient maintenance and improved utilization. To keep costs low, even the highest-end systems can be built out of small, low cost clusters made from standardized, commodity parts. The PSOs should evaluate the use of Oracle RAC for their critical Oracle-based applications.

6. Oracle Maximum Availability Architecture (MAA)

The Oracle Maximum Availability Architecture (MAA) is Oracle's best-practices blueprint that is based upon proven Oracle high availability technologies and recommendations. The goal of which is the removal of the complexity in designing the optimal high availability architecture so as to maximize systems availability at the lowest cost.

MAA reduces the implementation costs for a high availability Oracle-based system by providing detailed configuration guidelines. The results of performance impact studies for different configurations are highlighted to ensure that the chosen high availability architecture can continue to perform and scale accordingly to business needs.

MAA provides best practices and recovery steps to eliminate or minimize downtime that could occur because of scheduled and unscheduled outages as a result of human errors, system faults and crashes, preventive maintenance, data failures, corruptions, and disasters. MAA gives the ability to control the length of time to recover from an outage and the amount of acceptable data loss under disaster conditions, thus allowing the mean time to recovery (MTTR) to be tailored to specific business requirements.

7. MAA Components

a) Real Application Clusters - Real Application Clusters (RAC) enables near instantaneous instance and host failover. Combined with a connection failover implementation, RAC enables clients to transparently failover in seconds.

b) Oracle Data Guard - Oracle Data Guard manages a synchronized copy of the production database at a secondary site for protection from server/site outages. Data Guard manages the two databases by providing remote archiving, managed recovery, switchover and failover features. Data Guard provides the following benefits:

- Disaster Protection
- Protection from human errors

- Protection from data failures
- Capability to use the standby database for reporting
- No data loss or minimum data loss options
- Offload backups at the physical standby database for production database recovery

c) Redundant middle or application server tier - The Application Server tier consists of a set of servers that provide application services to the clients. The overall application tier functionality may be distributed across multiple host machines. In most cases, the middle tier applications are stateless and high availability is maintained by having server farm clusters of identical middle tier hosts providing the same key functionality.

d) Redundant network infrastructure - A highly available network infrastructure may include redundant devices such as DNS servers to route between primary and secondary sites, load balancers to route to any available application servers, load balancers to route to any available database node in the cluster, and physical layer switches.

e) Redundant storage infrastructure - All hardware components of a storage array must be fully redundant, from physical interfaces to physical disks, including redundant power supplies and connectivity to the array itself. The complete storage is replicated at the secondary site for adequate data protection.

f) Sound operational practices - An architecture that contains all the necessary hardware and software features without sound operational practices will ultimately fail to meet availability service levels. Operational best practices provide the greatest impact on availability by preventing or detecting potential problems and recovering from outages within a pre-defined MTTR.

I. Backup & Restore

Backup and Restore defines a combination of technology and methodology for preserving and recovering data that is stored on mainframes and other servers. A myriad of commercially available systems exist that span the range of low cost tape backup to the more sophisticated and expensive disk-based backup. Beyond the cost of the systems, supporting network infrastructure, skilled employees and defined processes of recovery and backup are necessary components of the total package. Organizations should evaluate the network bandwidth that is needed, server processing power that is required, and the impact that the organization's disaster recovery strategy has on Backup and Restore. The following sections enumerate best practices in several areas related to Backup and Restore.

1. Tape Systems

- Tape systems provide the best medium for long term and off-site storage. This makes tape an important consideration for disaster recovery and business continuity planning.
- Tape provides optimum durability (can survive large drops and tolerate rough handling).
- Tape offers a low unit cost per megabyte.

- Backup tapes should be stored in an off-site storage vault as the preferred alternative to a safe deposit box, another corporate location or an IT manager's home.
- Daily vaulting is required for critical applications.
- When evaluating tape vaulting service providers, the following factors should be considered: theft deterrence, fire protection, flood protection, environmental control and 24-hour access.
- Backup tapes should be analyzed occasionally to see if they produce errors in order to ensure that they will execute properly when needed.
- Review and assess the impact of failed tape jobs.
- Staff needs to be trained in Backup and Restore operations to prevent failed operations or misplaced media.
- Off-site contracts allow up to a 5% loss of media. Best Practices dictates less than 1% loss.
- Backup requirements include: adequate tape drive speed and capacity, adequate network bandwidth and backup server processing power.
- The backup window has diminished (due to 24x7 availability needs; therefore, systems must perform backup at shorter intervals while additionally being able to optimize and tune as required.

2. Disk-Based Systems

- A high performance data protection strategy can integrate both disk and tape storage in order to meet stringent high availability requirements and maintain critical service level agreements.
- Disk-based backup and recovery operations help administrators improve performance substantially over traditional sequential tape-based backups while offloading the host CPU to help increase system availability for business-critical applications.
- Backups can be performed quickly from a primary disk to a backup disk and then copied to tape.
- Disk-based backup provides "snapshots" of data at specific points in time.
- Five methods of disk-based data protection are currently available and can satisfy a multitude of application backup requirements: a) backup to disk, b) disk staging, c) inline copy, d) synthetic backup, and e) instant recovery.

a) **Backup to disk** - The backup-to-disk approach writes the same data to a file on a disk volume as it would to a file on a tape volume. When a backup-to-disk operation completes, a single file the size of the backup will exist on the target volume that contains all the files that were backed up.

b) **Disk staging** - The disk staging method writes backup data to a disk cache before sending the data to its final destination, whether it is disk or tape. Disk staging enables administrators to complete backups faster, shortening the backup window and thereby affecting business applications less than a direct backup-to-tape method.

c) **Inline copy** - The inline copy method writes backup data simultaneously to multiple destinations, such as disk and tape, thus combining backup and duplication as necessary.

d) **Synthetic backup** - When system availability requirements do not allow enough time to complete a full backup, administrators can create a synthetic backup that is identical to a current full backup. A synthetic backup assembles data from the system's previous full backup and subsequent incremental backups without involving network resources.

e) **Instant recovery** - The instant recovery approach helps deliver the benefits of disk-based data protection without the need to perform backups or recoveries over the network. By restoring data from snapshots residing on a local disk, administrators quickly can resolve application corruption and end-user errors such as accidental deletions and overwrites.

3. Backup/Restoration (B/R)

- Risk and labor are intertwined to the extent that, to reduce risk, companies must review and assess the impact of failed tape jobs daily to determine whether any critical jobs must be restarted immediately.
- Backup tapes (or duplicates) should be unloaded from the tape library and moved to an off-site vault daily as a best practice. Of course, the tape library must also be reloaded with fresh media.
- B/R is an inherently labor-intensive effort; its use manifests other problems, particularly in smaller, remote offices. Often, these offices do not have IT professionals available to manage B/R operations.
- Especially during periods of turnover, the Backup/Restore staff might not be schooled in B/R best-practice operations. The result can be misplaced media, mislabeled media, failure to execute necessary operations, and an inability to troubleshoot and solve technical problems. Moreover, remote sites rarely seem to create duplicate media and move it off-site regularly. All these factors in combination make a lost/unrecoverable data situation a virtual certainty.
- As a removable media, tape also represents a vulnerability to data security. Although most off-site vault suppliers are bonded and insured, many supplier contracts allow up to a 5% loss of media elements without penalty (META Group best practice dictates a less than 1% loss). Such media loss is unacceptable for two reasons.

- The loss of a single critical piece of media could prevent the restoration of an entire system.
- Given current regulatory requirements regarding privacy, the unauthorized disclosure of sensitive information could expose the organization to significant legal liability. With the large capacities of disk libraries and the inherently higher reliability of disk as a medium, the impact of failed tape jobs (during the "buffering stage") now approaches zero. Once data is moved to a tape-based archive environment, however, it is once again subject to these potential media failures/losses.

- A key reason for ITO dissatisfaction with B/R systems is the difficulty in meeting the backup window.

- Because many systems commonly require 24x7 availability, the backup window has literally disappeared. Systems must be kept continually operational (e.g., repaired) without negatively affecting the core mission.
- B/R systems are surprisingly difficult to optimize and keep in tune. As data volumes continue to grow at a 40%-45% compounded annual rate, tape systems gradually run out of capacity. Other tuning problems require the following:

- Include adequate tape drive speed/capacity
- Network bandwidth
- Backup server processing power
- Disk drive controller throughput

- Any inadequacy of an individual component can result in backup failures, yet identifying and solving the problem can be time consuming.

J. Network Operations & Management

This is a critical area that must be in place prior to any major implementation of technical infrastructure. It is also a focal point in any network strategy and specific alignment to the ISO FCAPS (International Organization for Standards/Fault, Configuration, Accounting, Performance and Security) model is required. The key components in this area are the Management Layers and the FCAPS Processes.

The Management Layer depicts the Business Functions that drive the requirements and also the Enterprise and Element platforms that house the required tools, monitoring and alarming equipment. Additionally, the Service Layer, the last piece of the Management Layer, defines the Service Layer Agreements required to sustain customer satisfaction. The FCAPS processes support the Enterprise and Element Layers and define the fault, configuration, accounting, performance and security needs required to provide a seamless and high-performing platform.

- Organizations derive the most possible benefit when they utilize the ISO model of network management, known as FCAPS (Fault, Configuration, Accounting, Performance and Security).
- Database of all installed equipment and configurations; toll-free telephone support; supported monitoring.
- 24x7 monitoring of dedicated servers and network equipment (note both frequency and method, such as PING, Simple Network Management Protocol (SNMP); combination of Enterprise and Element Management Systems.
- 24x7 monitoring of the health of the equipment with alarms (homegrown/outsourced) and pager alerts for network failure and fail-over; 24x7 monitoring firewall services available.
- Alternate Network Operating Center available as required.
- Second-tier support personnel (based on Tier Level expertise); Trouble ticket processes.

- Logging for all unusual or unexpected events; automated case escalation procedures in place including escalation time frames; reporting that provides trending statistics on trouble tickets and minutes (above) to facilitate quality and customer reports.
- Configuration and Trending analysis for application implementation.
- Performance reporting and end user impact monitoring; periodic and exception reports provided to customers (including usage and problem reports).
- Spare equipment on site for key networking equipment available in case of hardware failure
- Business continuity plan/Disaster Recovery defining the Data Center needs.
- Daily site backups should be performed.
- Tape vaults or other secure storage facilities on site in case of natural disaster.
- Onsite and offsite storage available.
- Customer callout and escalation database.
- Communications systems (IVR/Voice/Intercom systems).
- Customer documentation on alarm handling.

The top tier encompasses the Enterprise view and ties together the alarms and faults from the second tier, the Element platforms. The Element systems are normally proprietary and very specific to the technology it is overseeing (i.e. fiber, applications, routers, etc.). However, it is very important that the alarms from these proprietary systems are correlated in one place, the Network Operations Center.

K. SCADA Support

SCADA support, as related to Information Technology, has unique requirements both in the skills required to maintain the platforms and the technologies needed to support the systems. The uniqueness includes specialized equipment (e.g. RTU's and Turret consoles) and specific, targeted applications for oversight of Energy Management and Distributed Management platforms.

Although SCADA systems generally perform only supervisory control and data acquisition functions, they are usually required to operate 24 hours per day 365 days per year. This differentiates them to a large extent, from back office applications where availability and reliability is not as critical to the business. If a SCADA system crashes, it can put the reliability of the electrical network at risk. Moreover, all data presented to the user by a SCADA system must be both accurate and on time. The following items enumerate best practices in several areas related to SCADA support.

- Refresh Policy for RTU's should be in place to address antiquated equipment. Many organizations do not allocate part of their budget to replace equipment and allow equipment to become antiquated.
- Ensure that there is information on the installed base that is documentation and stored in a database.
- Document the Configuration using Configuration and/or Asset Management software.

- Antivirus, firewall, and intrusion detection solutions are available and should be implemented. When implemented at various external and internal points of the cyber infrastructure, electric utilities can quickly recognize and stop malicious code and hack attempts.
- Monitor security efficiency and performance to ensure a robust security program.
- Periodically review and update emergency plans to include newer threats and vulnerabilities, and test these plans regularly.
- Logging and reporting should be enabled on routers and firewalls to gain a better understanding of remote systems and user access.
- For real-time data acquisition (SCADA), direct links to each RTU (or critical RTUs at a minimum), in addition to receipt of data from local control centers should be required in case EMS-to-EMS control center communication go down.

1. Real-Time Attributes

Real-time data storage is at the heart of any SCADA system. The term database is often used in this regard, but this terminology can be a little misleading since the word database has come to be accepted for long-term historical storage of data in a much broader context. The SCADA offers instead, a real-time database to describe instantaneous values of all configured plant input/output (I/O) signals or tags. In addition, the real-time database will usually include any derived tags used to contain results of calculations performed on process plant variables. Key attributes of any real-time SCADA database are:

- **Capacity** - the total number of points that can be configured into the real-time database.
- **Performance** - how efficient is the run-time performance of the real-time database. Speaking typically in throughput in the order of thousands of changes in data per second, the delay associated with storing or retrieving a value should be as short as possible.
- **Configurability** - once a SCADA system has started up and is monitoring and controlling a process, it is inconvenient to have to shut it down to make minor modifications to the system configuration.
- **Extensibility** - a real-time database should be able to accommodate record structures defined by a system integrator.
- **Networkability** – real-time SCADA databases should be locatable on potentially any computer node in a networked environment. A corollary of this requirement is that it must be possible to distribute a large database across as many or as few nodes as is appropriate to the user. This distributed nature should in no way complicate the configuration, nor compromise the performance of other SCADA functions.

L. Capacity Planning & Performance Management

The importance of, and interest in, capacity planning best practices continues to grow, resulting from evolving operational maturity and more pragmatic spending for infrastructure expansion. Users are moving away from simple measurements (sometimes subjective hunches) toward more enhanced capabilities that extend the rigorous capacity planning processes of mainframe

environments to the distributed, networked application world. Common triggering methods and simple trending analyses inadequately assess changing requirements. A more sophisticated capacity planning process that includes infrastructure and application behavior modeling across platforms is often necessary. Historically, siloed efforts have hampered end-to-end performance modeling (i.e. network without application planning or vice versa), but software vendors have expanded their horizons to encompass a fuller domain of infrastructure and applications to reflect the growing demand for these products. A good practice is to initiate merged capacity planning efforts using processes that span technology silos. Tool deficiencies will soon give way as vendors rapidly expand their offerings.

M. Project Management and SDLC Methodology

1. Project Management

Project management is the application of knowledge, skills, tools, and techniques to plan, schedule, and control project activities to achieve the performance, cost, and time objectives associated with the project. Managing projects successfully requires taking control of the tasks and ensuring that they are completed with the least amount of effort, expense, and risk.

A defined methodology for project management should be adopted by the organization, and appropriate training conducted for project participants. All technology related work effort conducted by the organization should adhere to this methodology, regardless of project size (cost, resources, or scope), duration, or complexity.

The project management methodology should include defined processes, work product templates, and standards or guidelines for the following functions:

- Project Planning
- Project Tracking and Reporting
- Project Control
- Project Completion

a. Figure 31 – Project Management Processes

Project Planning		
Process	**Work Product**	**Standard or Guideline**
Create Project Definition or Statement of Work	Project Definition SOW	The Project Definition/SOW should contain the following: • Project Background • Project Objectives • Scope • Project and Management Approaches • Deliverables • Timeline/Initial Project Plan • Roles and Responsibilities • Assumptions • Risks • Project Completion Criteria • Costs

Project Planning

Process	Work Product	Standard or Guideline
Create Work Breakdown Structure and Define Project Tasks	Work Breakdown Structure Project Plan Outline	The Work Breakdown Structure should decompose the project's work and cost into logical components (phases, sub-phases, major activities) that are defined by the organization's IT SDLC methodology. Project Tasks should be defined for each activity, and again, be initially defined based upon the methodology.
Estimate Work Effort, Resources, Task Dependencies	Project Plan - Initial Project Estimating Guides Resource List	For each task, Work Effort should be estimated, and Resource Types defined for each one. Work Effort is generally defined in hourly or daily increments, and should be no greater than 40 hours/5 days. Estimates should be derived using both top-down and bottom-up approaches. Different estimating techniques may be used depending upon the size, complexity, known scope detail, methodology phase, previous experience, etc. Such techniques include: comparative, expert judgment, proportional, widget counting, and function/feature point analysis. It is best to use at least two different techniques for validation. The IT organization should define standards for estimating techniques. Tasks should be linked to dependent tasks to create the critical path.
Create Project Plan and Staffing Plan	Project Plan - Final Staffing Plan	An automated Project Planning Tool should be used to create the detailed Project Plan. All tasks, assigned resources, work effort, dependencies and milestones should be defined. Once completed, a project baseline should be created. The Staffing Plan should detail the project resources required to support the project, and should be listed by functional or skill type when specific named personnel are not known. It is critical to define the time frames for each resource to ensure that the right skills are on the project at the correct times to accomplish the work without delays.
Develop Detailed Budget	Detailed Budget	The Detailed Budget should be linked to the work effort, resource costs, and duration defined in the Project Plan. Project support costs, travel, equipment, and contingencies should be applied where appropriate. When creating the Detailed Budget, it is helpful to capture assumptions that were made, so when these change, it is easier to perform change control from a documented baseline. Use the budget reporting functions in the project planning tool to assist in the creation of the Detailed Budget.

Project Tracking and Reporting

Process	Work Product	Standard or Guideline
Collect and Review Project Data and Update Project Plan and Budget	Team Member Status Reports Time and Expense Reports Task Assignment Schedules Project Plan Budget	The Project Plan should be reviewed and updated on a weekly basis by accumulating each Task Assignment update, Team Member Status Report, and Time and Expense Reports from each team member. Within the Project Planning Tool, Actual effort applied should be posted against the Baseline work effort and new estimates to complete tasks should be applied. Schedule, budget, and cost variances should be calculated.
Evaluate and Report Project Status	Project Status Report Dashboard Report	Review the Project Plan, Budget, Status Reports, Issues, Change Requests to evaluate the Project status to determine whether the project is on track to be completed on time, within budget. Create a weekly Project Status Report summarizing the work completed for the week, the planned work to be completed the following week, the status of milestones or deliverables, and summarized major project issues and risks. The Project Status Report may also contained updated cost to

Project Tracking and Reporting		
Process	**Work Product**	**Standard or Guideline**
		date information as well. This report is intended both for internal project control, as well as external client communication. The Project Manager should conduct weekly project status meetings with the team to review and resolve issues, and communicate information that is relevant to the project success. In addition, the Project Manager should conduct a weekly/bi-weekly project status meeting with the client sponsor. A color coded dashboard report should be created on a monthly basis to depict schedule status, budget, staffing status, issues, and watch areas. The colors (red, yellow, green) indicate relative degree of concern in each area. This report is generally sent to an oversight body such as a Project Management Office to be accumulated and rolled up into an overall enterprise-wide status for all work activity.

Project Control

Process	Work Product	Standard or Guideline
Control Project Issues and Changes	Issue Reports and Log Change Reports and Log	Throughout the course of the project, issues that could hinder the ability to meet the schedule and budget need to be captured in formal Issue Reports. Each report should define the issue, identify the person(s) responsible for resolution, due date, and final resolution In addition to issues, Change Reports should be used to capture any modification to the schedule, scope, resources, activities and costs of the project. Each report should define the change, identify the person responsible for analyzing the impact, cost and schedule impact, due date, final recommendation/resolution, and person responsible for reviewing and/or approving the change. To manage the list of all issues and changes, an Issue Log and Change Log should be created and tracked. The weekly and monthly status reports should provide a summary of the disposition of these issues and changes. The weekly status meetings should allot time to review these as well. Project schedules and budgets should be updated regularly to reflect the impact of both issues and changes. In addition, a formal issue escalation process should be defined and followed that would categorize issue/change types that need to obtain management or project oversight board review and/or approval.
Manage Project Risks	Risk Mitigation Plan	Project risk management aims to identify the areas impacting the successful completion of the project that need to be closely monitored. This can be an effective process for the project manager to escalate issues that need mitigation. Risks can come from a variety of sources (e.g. technical risk, resource dependency risk, scope creep, interdependency with other projects etc.) and each one must be considered. The risks should be identified, documented, analyzed for cost and schedule impact, and ranked according to severity, control, and probability of occurrence. Risk mitigation strategies should be implemented for those items with the highest risk score and reviewed with management and/or project oversight board.
Manage Resources	Staffing Plan Team Member Project Expectations Project Administrative Policies and Procedures	At the onset of the project, a Staffing Plan is created to define the resources by specific skill sets, tasked assigned to the resources, projected hours required, and schedule of when the resource is expected to participate in the project. This Staffing Plan should be monitored regularly to ensure that the appropriate resources are available to meet the successful completion of the project. The Staffing Plan should contribute to the overall Resource Management function of the organization, ensuring that organizational resources are utilized appropriately and efficiently. When resources are assigned to the project, the Project Manager should document Project Expectations for each team member. These should be reviewed with each member to ensure that the resource understands the tasks assigned, the schedule, work products and deliverables, and quality expectations. Orientation and training needs should be identified and scheduled. Project Administrative Policies and Procedures should be documented, distributed, and communicated with each team member, and updated and redistributed regularly. These policies include things such as vacation schedules, time/expense reporting, status reporting, regular meeting schedules, work times, etc.
Perform Quality Assurance	Quality Plan	Quality Assurance involves the review and audit of project activities and work products to verify that they are being completed in compliance with applicable procedures, standards, guidelines, and contract requirements. This function must occur throughout the project and ensure that the appropriate deliverables are being completed and any non-compliance is being escalated to the appropriate individual. QA should not be viewed as a means of providing insight to management

Project Control		
Process	**Work Product**	**Standard or Guideline**
		regarding the true state of a project. If this stance is taken, QA will be seen as an intrusion to the project and project personnel will be resistant to disclose information. QA should be viewed as a function that is aligned with the project team's objectives, namely, a mechanism to provide adequate confidence that the solution optimally fulfills the business requirements and customer expectations. The Quality Plan describes what quality is for the project and how it will be achieved via the creation and application of standards, procedures, and tools. It defines roles and responsibilities for team members, as well as quality measures. The Quality Plan also outlines the processes and techniques that will be used to verify that the standards and procedures are being met. These include: record keeping, self-checks, peer reviews, walks-through, workshops, formal reviews, and internal/external audits. The Quality Plan and its components should be part of either an orientation or training session.
Manage Project Documentation	Document Repository	Project Document management is started at the onset of the project, and should be regularly administered during the course of the project. A Document Repository (physical and electronic components) should be created to house all project information. It should be centralized in one place, and easily accessible by project team members. Electronically, the Repository should be accessible from any location, at any time. Appropriate security is required, and documented standards and procedures should be followed. A logical taxonomy should be standardized and used throughout the organization for each project. Back-up and recovery procedures should be regularly executed, and required data archival rules followed.

Project Completion		
Process	**Work Product**	**Standard or Guideline**
Obtain Project Acceptance	Acceptance Document	At the completion of the project as defined by the obligations specified in the SOW, a formal Project Acceptance procedure is executed (generally this has been specified in the SOW), and an Acceptance Document created and signed by the Project Sponsor.
Gather Project Performance Metrics	Performance Metrics	Review the Project Plan, Budget, Status Reports, Issues, Change Requests, and other Project Documentation to gather relevant project performance Metrics (i.e. actual development time for a complex function developed in X technology took on average 32 hours). Account for differing skill sets, learning curve, and other circumstances. Compile this information for the purpose of creating future estimation models, proposal/SOW cost and schedule estimates, etc.
Conduct Sunset Review	Sunset Report	After the completion of the project, conduct a Sunset, or "Lessons Learned" review with the project team members to understand what went well during the project, and what areas could be improved upon in future projects. Compile recommendations and corrective actions, address where possible, and constructively communicate to relevant parties throughout the organization.

2. SDLC Methodology

A systems development life cycle (SDLC) project delivery methodology is a set of proven processes, standards, practices, deliverables, templates, and tools that an organization utilizes in completing different types of IT projects. These elements have been designed and developed to work in concert with each other, thus providing greater business value than if the elements were used on their own. A methodology ensures that individuals and project teams can accomplish their work in an efficient and effective manner while at the same time contributing to the overall efficacy of the organization.

Most methodologies are comprised of project phases, sub-phases, activities, tasks, deliverables and work products, responsibilities, and project control functions. In addition, since many projects are conducive to iterative design and development, many methodologies accommodate a modular approach that allows component parts to be repeated in an efficient manner. Some of the main benefits of a methodology are the following: The following benefits accrue to organizations that follow a defined methodology:

- Repeat delivery of projects on-time, on-budget, and with a high degree of quality across all projects.
- Ability to create and leverage best practices across the organization.
- Clear definition of roles and responsibilities.
- A set of guidelines and project roadmap that improves the ability to plan, estimate, cost, track, and report on all projects.
- Ability to create a common language between the project team and its sponsors to facilitate greater communication and alignment.
- Mechanism to facilitate and encourage the reuse of generic components, thereby reducing time and costs.

Historically, methodologies were created to manage the planning, analysis, design, development (coding), testing, integration, and deployment of systems or applications. Many methodologies did not accommodate non-system development projects such as IT Strategy and Planning, Assessments, Technology Evaluation and Selections (software and hardware), Process Improvement (BPR, Six Sigma) etc. Hence, many IT organizations that do not do in-house application development do not believe that they need a methodology. This is not true; all IT Organizations need to create or acquire a methodology, regardless of their defined role or internal service offerings. Modern methodologies accommodate different functions that an IT organization may perform, and are generally adaptable to handle custom requirements.

A new organization that will undertake a considerable amount of IT related projects (i.e. start-up of new RTO) should consider purchasing a methodology, rather than expending the resources to develop its own.

When selecting the methodology, ensure that it is flexible enough to enable its technology partners to conform to it, without radically changing their own processes. This can be accomplished by defining the elements that have a proscribed format (e.g. deliverables) while allowing latitude in some elements where uniformity is not as critical (e.g. the vendor's actual development process). In addition, if the organization is not going to perform a large amount of in-house application development, select a methodology that is strong in the areas of IT

Planning, Requirements Definition (Analysis and Design), Technology Selection and Installation, Systems Integration, and Testing (particularly integration and performance).

Having a methodology is not enough; standards, templates, and guidelines should be in place as well. Technology vendors must conform to these. The methodology should be communicated and enforced throughout the organization, with appropriate and timely training provided.

N. Engineering Review Board

The Engineering Review Board (ERB) is a necessary forum in order to provide consistency, credibility and checks and balances when applied to technical platforms, technical designs, specifications, projects, etc. The ERB is usually composed of representatives from the major technology organizations so that the proposed solution is holistically reviewed to ensure that it conforms to the technical standards that the organization has established. The ERB process requires the preparation and distribution of documentation that provides a methodical and overall presentation of the tasks, solutions, conclusions and recommendations. In order to avoid confusion, misconceptions and the "reinvention of the wheel" syndrome, a boilerplate format for the submission of documentation to the ERB is required. The following sections depict a general table of contents and section description that should be part of the ERB documentation:

a. 1.0 Overview

The purpose of this section is to present a complete background regarding the subject matter of the document. It is an expansion of the information presented in the Introduction of the executive summary. In reality, it is normally generated before composing the executive summary. In fact, the executive summary will most likely contain a condensed version of the overview presented in this section

Remember that the overview should capture the total picture, or "systems" approach, with regards to the design, problem solution, process or other types of subject matter. This approach documents and helps the reader to understand the scope of the effort. A project or initiative with substantially narrow scope may justify why a Fast Track ERB is pursued.

b. 2.0 Goals/Objectives

It is very important to properly articulate the overall goals and objectives of the project. This can be best accomplished by providing statements which address the importance of the project, the final result, a tentative schedule and a specified budget. In many cases the overall project goal is an opportunity for the author to champion an idea, design, project or other subject matter targeted for the ERB review.

The deliverables help to define the completion of the proposed activity as defined for the ERB, whether it is a project, application, architecture, design or other. At this point, there should be no scheduling or sequencing of the deliverable(s). Through the definition of the deliverables, the major milestones should be identified.

c. 3.0 Assumptions and Risks

This section is used to present underlying assumptions around a design, project, procedure, etc. Normally, in order to accomplish the previously stated goals and objectives, one or more assumptions are made. In most cases, assumptions are usually aligned with technical, logistical or budgetary considerations.

This section is also used to define any "must" criteria associated with the completion of the task as presented in the document. The "musts" are similar in nature to the other requirements; however, they are significantly important and should be identified with a separate heading.

In general, there is always a risk associated with undertaking a technical project. Similarly, there may also be a risk in doing nothing. With this in mind, it is important to articulate any potential risk(s), even if they appear academic in nature. Clearly, risks which can significantly impact the subject matter of the document must be discussed in detail. It may be helpful to present "what-if" scenarios in order to identify potential risk conditions.

Often times, imposed or must conditions are what drives the need to engage in the Fast Track approach. Furthermore, these "control" conditions may lead to a final state based upon larger or perhaps broader assumptions because sufficient time or conditions reduce the available time for diligence.

d. 4.0 Strategies and Methodologies

The purpose of this section is to identify the overall (systems) process for accomplishing the goal(s). If unique or creative types of processes or methods were used to solve a problem, as opposed to a predefined "cookie-cutter" method, the author should describe their proposed approach. For example, does the design require throwing away previous established standard?

If the document addresses a design or project that has strategic value or benefits, an explanation is appropriate. Also, if negotiation of services or application development is required as part of the design or implementation of a strategic project, the strategy should be documented.

If a business case model or analysis has been prepared it should be referenced in this section. The identification of the financial methodology used (where applicable) should be spelled out. Reference must be made when process methodology tools are required to complete activity related to the presented subject matter.

e. 5.0 Implementation Considerations (Impacts, Issues, etc.)

Of particular importance is when the ERB document deals with subject matter which has potential for impact to global organizations horizontally across the corporation. The author is to identify significant issues and considerations that must be fully addressed as part of the plan. In order to accomplish this requirement, a well thought out plan which employs the essential project management components must be utilized. Through this process, the proper planning will have been accomplished to mitigate the potential impact issues.

In many cases, implementation concerns or issues arise due to either a new design or modification to an existing system which potentially can result in some level of impact to system operation. It will be helpful if the author performs some degree of contingency analysis (i.e. "what-if" scenarios) to help surface any potential impacts or concerns (technical and/or cost related).

For Fast Tracking, it is important to capture any impacts, issues, risks, etc. that may be directly attributed to the fact that a fast-track approach was enacted. Again, if time pressures warrant fast tracking, then usually there is an added element of risk presented. Implementation also tends to become much more of a logistical issue when faced with imposed time constraints.

6.0 Technical Alternative Analysis

In most cases, this section will constitute the bulk of information to be conveyed. When a design (new or modification) is being presented, comparative analysis from a technical/operations perspective must be provided. For procedures, processes, etc., an explanation which addresses why it is required (as opposed to doing nothing) should be conveyed.

In the case of technical designs or modifications, a minimum of three (3) alternatives should be presented. In all cases, the alternative which considers a "do nothing" scenario must be addressed. It is important to elaborate on this alternative because it can occur unintentionally from a deadlock or lack of decision-making process. Ideally this condition can be quantified in terms of cost and/or business impact. If a single solution condition exists, then sufficient background and explanation must be generated to substantiate this condition. References to cost impacts due to technology alternatives can be made to assist in clarification and support of technical alternative discussion. When considering and evaluating various alternatives, a systems level focus of the problem that considers migration, integration and impact issues and strategies is suggested.

The Fast Track process may have a direct correlation with the level and breadth of alternative analysis. In many cases, constraint time to implement a project or design will dictate the number of alternatives considered. Similarly, if the Fast Track is being utilized because of the limited scope of the project, then again the alternative analysis may be quite brief. Consequently, a Fast Track approach will often reduce the content of this section considerably. However, maintaining the "as-is" state should always be addressed as an alternative.

f. 7.0 Project Management Documentation (applies to project-oriented ERB)

This section of the document is used as a central place holder for associated project management documentation. A list of the key required documentation is presented below. Additional project management related information may be required depending upon the scope and financial impact of the subject matter.

- Work Breakdown Structure (WBS) that captures the major activities (work packages) that are required to complete the project or effort being presented. The WBS is most effective when presented in graphical format using a hierarchical format similar to an organization chart.
- Responsibility Matrix identifying organizational structure such as a person, contractor, Division/Dept., etc. (resources) as rows of the matrix (spreadsheet). The columns of a spreadsheet identify the WBS activities. The cells where rows and columns intersect would contain text and/or shading to identify which resources have primary responsibility versus involvement or some level of effort.
- Project Schedule showing beginning and end times, major milestones and activities. Depending on the level of effort and number of overall activities identified in the WBS, a schedule indicating WBS level 2 summaries is appropriate.
- Cost estimations and analysis where and when applicable that correspond to technical alternatives. A cost estimate (budgetary or better) is required for ERB documents that propose new or modified system designs, projects, etc. Vendor proposal(s) are normally required, where applicable, to meet this budget or better estimate objective. The cost estimate should include NPV analysis to capture the time-value associated with money where applicable.

- Fast Tracking an ERB may indeed be required for a fast tracked project. For this situation, the project management content and documentation becomes critical. The success of fast tracking is highly dependent on project management methods. This section perhaps becomes the most important and scrutinized portion of the ERB document for fast tracked initiatives.

g. 8.0 Financial/Cost Evaluation

An explanation of the financial and cost considerations, business case development, cost analysis and evaluation related to the ERB subject matter is to be presented in this section. Cost estimations supporting the discussion will be included in Section 7.0. Additional supporting financial documentation such as NPV analysis is to be included in this section. Any assumptions, special conditions or other considerations dealing with cost related issues are to be presented. Adherence to corporate finance procedures for financial analysis must be consistently applied.

The importance and precedence of cost may need to take a back seat to implementation considerations during Fast Track projects and efforts. Consequently the level of detail, diligence and content associated with cost analysis may be significantly less than a normal effort. With this in mind, the ERB documentation as presented for a Fast Track ERB may lack detail. There are however, situation in which the ERB is being conducted for a design, project or otherwise that places major emphasis on cost. This condition will add additional weight to the cost component thereby creating significantly more work and detail on the cost evaluation portion of the solution.

h. 9.0 Decision Analysis and Process Methodology

Note: The Decision Analysis does not need to be extensive at this stage, but must at least depict alternative solutions were considered.

When a formal decision, problem or process methodology is utilized for analysis, recommendation and conclusive purposes, the appropriate corporate standards for these methods must be applied. In many cases, these tools include the Decision Analysis. This section must include the documentation in the prescribed format when these tools have been employed. The major objective of this section is to provide the substantiating and supporting analysis and information to support the conclusion and recommendation(s) as indicated in the executive summary portion of the ERB documentation package.

O. Problem Resolution and Management

As the PSOs perform data center operations, support applications and manage the network, it is inevitable that problems will occur. It is important that the IT organizations have defined problem management and problem resolution processes to deal with these situations. Problem Resolution and Management encompasses the detection and processing of significant events occurring within the Information Technology platforms. The process should start with event detection and notification and then migrate to isolation, diagnosis and resolution. Proper tracking throughout the process along with customer verification will complete the process.

Good practices follow the FCAPS model and in particular, the Fault Management module. Proper alignment to this model allows events to be correlated and filtered before information is forwarded to the proper support agency. This process minimizes duplication of tickets and response efforts. Tracking can now begin with ticket creation, ticket correlation, status documentation and resolution verification of the reported problem. This process ensures the documented resolution is working and meets customer's expectations.

The tracking system will eventually consist largely of a sophisticated workflow engine. This system will receive, store and process information related to problems automatically. Automated trouble ticket generation will eventually be used as a method to promote the ease of use of the trouble ticket system, provide accurate/historical records of the problems and reduce errors that is usually the result of manual ticket generation. Notification is the next key component of this problem resolution along with verification and escalation as required.

P. Root Cause Analysis

Root Cause Analysis is a process that is related to the problem resolution and problem management processes. When a significant problem occurs, management should determine whether a Root Cause Analysis is warranted. The Root Cause Analysis process should be designed to determine what the root cause is and what all of the contributing causes are. Contributing causes could be related to technical, managerial, communication, process, or procedure issues.

VIII. Appendix B - Technical Risk Management / Technical Risk Assessment

A. Introduction

Technical Risk Management can be defined as the process of analyzing an organization's exposure to risk as a result of technology implementation and determining the optimal methods to handle such exposure. Gestalt has developed a model that divides Technology Risk Management into four discrete segments: 1) Administration and Processes; 2) Prevention, 3) Detection, Identification and Containment, and 4) Assessment, Correction, and Recovery. This model is based upon the following premises:

- Threats exist from internal persons, external persons and naturally occurring events. Preventive actions are required to reduce the probability of unwanted attacks and events.
- These potential attacks and events have various effects on financial, productivity, public relations, customer satisfaction, and other values or goals.
- Quickly detecting and identifying the source of the attack or event and then containing them enables the organization to reduce the duration of the attack or event.
- Accurately assessing, correcting, and then recovering to the point that existed before the attack or event is critical to restoring the organization's services and to reduce the duration of the attack or event.
- Administrative controls and processes need to be put in place a priori to govern the other segments.

In the Prevention section, policies regarding software backdoors in vendor software, data validation, database security, test data security, software usage, external network integration, home PC use, non-repudiation, remote access, and wireless networks, server access, Internet user registration, password resets, and password reuse should be addressed. Physical security should be addressed unless it is already covered in the facilities organization policies.

Policies regarding the Detection, Identification & Containment and Assessment, Correction, & Recovery are generally addressed via operational policies and procedures. Since they are critical components to the overall security strategy, the organization should ensure that they are developed, implemented, and followed.

Detection procedures governing Application Security, Data Security, Data Anomalies, Desktop Management, Virus Quarantine, Network Access, Network Log Analysis, Network Monitoring, and Physical Security should be addressed.

Corrective procedures covering Application Security, Data Security, Database Backup and Recovery, Off Site Tape Storage, Desktop Management, Virus Remediation, Network Access, Network Management, Physical Security, Server Administration, Virus Remediation, and User Administration should be addressed.

The Security organization should then perform an overall Risk Assessment and in areas where preventive actions are more difficult to achieve, ensure that more robust detection and corrective

procedures are established. Similarly, in situations where the impact and effect is large and is difficult to contain through detection and corrective procedures, greater preventive measures should be established.

The following sections discuss specific areas of Technical Risk Management that should be pursued.

B. Disaster Recovery

Every business and organization can experience a serious incident which can prevent it from continuing normal operations. This can happen any day at any time. The potential causes are many and varied: flood, explosion, computer malfunction, accident, grievous act, etc. The information below is designed to help PSOs properly plan for these scenarios. They will target reducing both the risk and impact should the worst occur.

1. Disaster Recovery Service Levels

Organizations should classify their applications and architecture according to their criticality to the organization. The following are class examples as defined by Service Providers (Gartner Group, Meta Group).

a) Class 1 critical application services, with RPO and RTO from minutes to an hour or two, most enterprises invest in a replicated architecture in an alternative facility.

b) Class 2 services offer RPO of four hours and RTO of less than a day; meeting those requirements typically requires shadowing data to a recovery facility.

c) Class 3 offers standard tape recovery; these services are often outsourced.

d) The lengthier recovery times for Class 4 services, enables enterprises to reduce costs by contracting for quick ship services. In a disaster, systems are typically shipped within 24 hours of notification.

2. Disaster Recovery Best Practices

a) Disaster Recovery vendor prices vary so widely depending on the size of the company and scope of its requirements that no standard price range is meaningful; planners should request pricing for a consistent set of criteria from several Disaster Recovery vendors.

b) Ongoing review and testing of the continuity plan and recovery resources is essential, as the initial solution will change over time, depending on the company's reliance on rapidly changing technologies, the existence of manual workarounds for technological failure and each operation site's exposure to environmental risk factors, such as power outages and natural disasters.

c) The EPZ zone defined by federal regulations indicates that in a true disaster, a 10 mile radius must be established and plans of evacuation should be in place. It is critical that that Primary and Alternate sites receive immediate design attention that splits these sites appropriately so that both are not impacted.

d) Storms conditions and regional outages can also play a factor in close proximity.

e) Point of Presence (POP) related to Carrier circuits is another issue when a corporation is seeking design criteria related to Disaster Planning. In most cases, dual POPs will be the

most effective method of eliminating risks associate with the loss of a critical carrier POP.

f) Disaster Recovery also dictates that decisions must be made concerning the type of site to be used as well in critical areas. The first key determination is that of defining the type of Alternate site that will be used in case of a disaster at the Primary location. The decision process is centered on whether or not the site will be a HOT, WARM or COLD facility.

g) Hot sites can demand major costs in that the same infrastructure (as Primary) is duplicated at the Alternate site. Server mirroring, clustering or similar technology is leveraged that allows for instantaneous and "live" data to be present at both the Primary and Backup facility. Business continuity plans and Impact studies must be conducted to be sure that less critical functions are not included in the data capture (that dictates more dollars spent).

h) Testing and back-out Planning (back to Primary site) is a necessary requirement.

3. Additional Areas of Risk

a) Project Fails to Involve Employees from All Business Units. Firms implementing IT security and risk management best practices include employees from all levels of the organization in risk management and disaster recovery planning. Failure to include employees from all levels and business units incurs two major risks: (1) inadequate or improper planning of executables and procedures and resources for those units and (2) lack of budgetary support from that unit for plan maintenance/testing.

b) Neglecting Review, Maintenance and Testing. Realistic testing of business continuity plans—so critical to recovery plan success—depends on the Executive Level support placed on business continuity. If executives fail to support testing with budget and resource allocations, they fail to understand the importance of up-to-date plans for their own business units. They need to be reminded that plans are often updated based on points of failure during a test. Also, it is critical to understand how to bring the system back after declaring a problem.

c) Committing to a Contract without Performing Due Diligence. Without due diligence, an organization may be captured by impressive vendor Web sites and vendor-managed demonstrations, resulting in unrealistic expectations of a vendor's reputation, capabilities, support, policies and level of execution. For example, even the best vendor may have higher priority clients (government, military, healthcare) in a particular region, putting another client's recovery at risk of delay.

d) Failure to read the "Standard" Contract Clauses Carefully. "Standard" business continuity contracts may contain traps for the client (automatic renewal clauses) and back-door disclaimers for the vendor (exceptions to the recovery time commitment). For example, a force majeure clause is commonly present to excuse a vendor from liability in the event it fails to live up to contract obligations due to an unforeseen event outside the vendor's control—one that could not be avoided by exercise of "due care." Contract should include clear examples of such events. Otherwise, there is the risk that the vendor could fail to perform for reasons within its control. Be sure to review the service contract with an attorney well acquainted with such contracts.

e) Concentrating on the IT Department at the expense the business. While the IT function is well positioned to act as a facilitator, IT serves the business operations. Planning efforts must take into account all aspects of business continuity—data, finance, buildings, communications, equipment, personnel, customer service, knowledge assets and so on. Otherwise, if the IT department is the only part of the company prepared for disaster, the result could be a nice safe data center but no way for the business units to operate or communicate with their systems.

C. Business Continuity

For many companies, a 4 to 24 hour site outage would cause irreparable damage to the enterprise. Consequently, many enterprises are incorporating Business Continuity Planning into their business process, application and technology architecture designs and building in continuous 24 x 7 availability. The risks are greater with SCADA environments, so the business continuity (BC) plan must address new scenarios and BC processes must integrate with a greater number of enterprise processes. The following are some best practices related to business continuity.

a) Must Perform a Business Impact Analysis to identify major risks. Not testing your plan or even more importantly, not performing a Business impact analysis (BIA) could be a critical mistake. Identify what the enterprise has at risk and which business processes are most critical, thereby prioritizing risk management and recovery investments.

b) Develop a matrix that relates applications and infrastructure in order to define all infrastructure needs for the Recovery Plan.

c) Prioritize critical applications for the recovery process.

d) Test the plan and be sure to include all people issues. Many business continuity plans have weaknesses where there is an insufficient emphasis on developing plans for the people side of recovery. A significant amount of preparation is required for the test; management of the event is also critical. Enterprises are placing greater emphasis on the impact of people issues, crisis management and forecasting/planning for additional scenarios, such as loss of life, lack of transportation and the complete destruction of facilities.

D. Security

While network security issues have always posed a threat to electric power system reliability, the expansion of remote access to SCADA systems, the rise of Internet access to business networks, and the rapid integration of legacy systems have significantly increased the number of potential system exposures. It is critical that companies/utilities work with government in establishing standards and practices related to Security in order to lessen the potential risks. The cost of implementation may not be low, but, the avoided cost associated with the mitigation of potential security risks would be well worth the expense. There will be a need for continued diligence and maintenance of the standards and practices, but, again the benefits of maintaining a robust security program far out weigh the costs. The following are some of the security best practices.

- Develop hardened Perimeter Protection (firewalls, filtering; secure online information).

- It is imperative that each organization deploy intrusion detection systems to guard against potential cyber attacks, improve procedures to guard against internet threats and enhance the security of on-line/application information.
- Citing past problems with computer disks and hard drives containing classified information, the government proposed that Nuclear and/or utility environments execute "an initiative to move to diskless workstations for classified computing" to allow sensitive functions to be performed in a more secure diskless environment.
- Budget and Execute 2 Security Audits per year; harden SCADA systems by removing unnecessary services.
- Develop on-going Circuit analysis for cost savings opportunities and removal of any gateways to the SCADA network.
- SCADA LAN access is limited, managed and adheres to documented security policies.
- Establish Policies and Conduct Training to minimize disclosing sensitive information.
- Caution using the web/Internet media (as proposed by some vendors) in the SCADA environment for controlling critical devices (i.e. RTU's) because of the continued instability of this platform (outages).
- An area of risk evolves around recruiting and training the best possible candidates for security jobs and to increase employee retention rates.
- There is often a need for "a change in the management culture" to improve the way the company accepts, analyzes and responds to criticisms and concerns from outside as well as from employees, who should be confident about raising questions or concerns without fear of retribution.

1. General Areas of Risk that must be defined:

- Identify sensitive information and critical systems.
- Incorporate local, state, and federal laws, as well as relevant ethical standards.
- Define institutional security goals and objectives.
- Ensure that the necessary mechanisms for accomplishing the program are in place with sufficient management support.

2. Specific Network Areas of Risk and Corrective Actions:

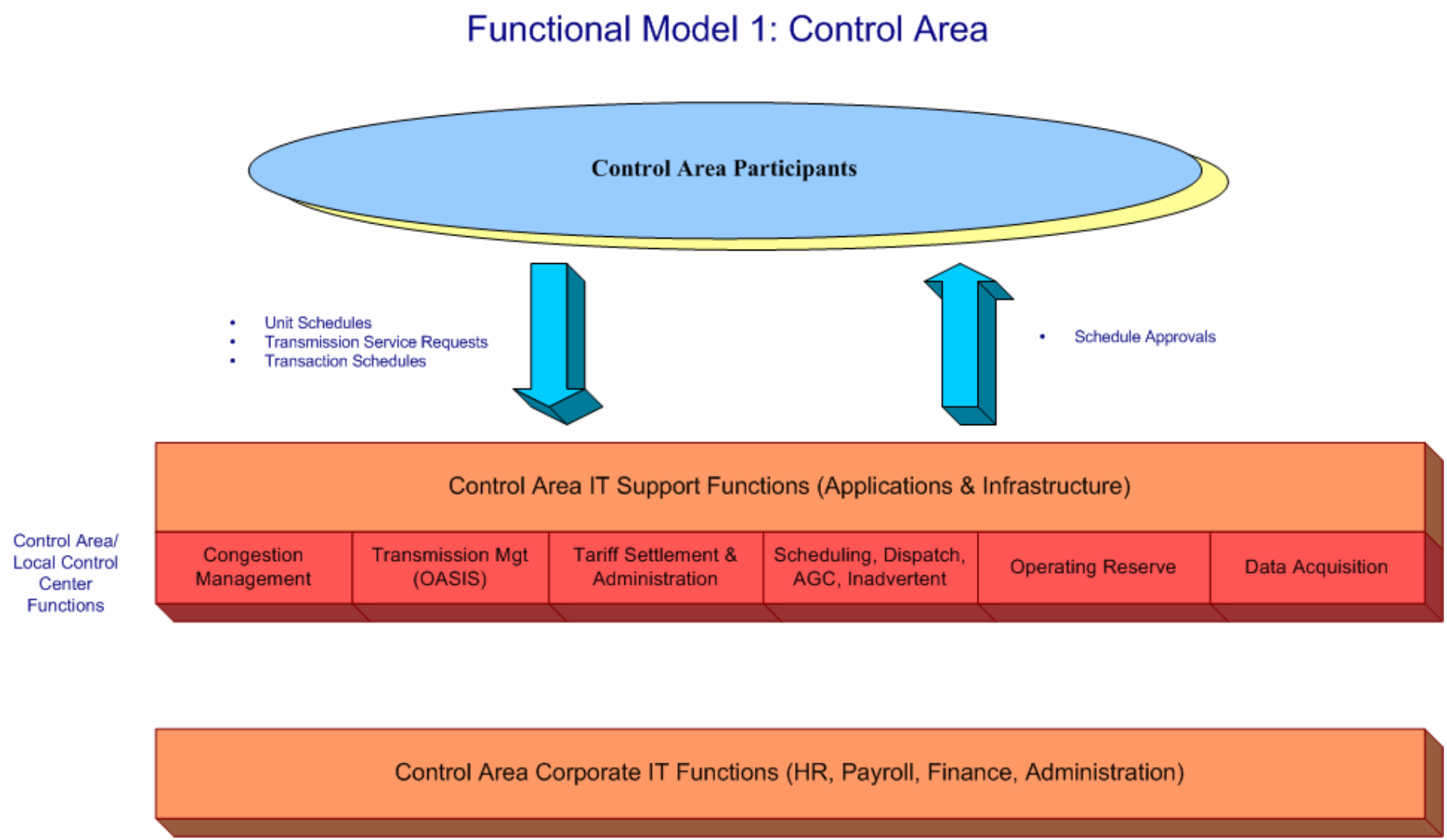
- Perimeter protection (firewalls, filtering router).
- Intrusion detection.
- Authentication and authorization (passwords, Secure ID).
- Backup and recovery systems to restore after a problem, such as load balancing, failover protection.
- Regular assessment of network infrastructure.
- Assessment of network expansions or additions.
- Tape or media storage offsite backup.

- Regularly scheduled security audits.
- Server anti-virus software protection.

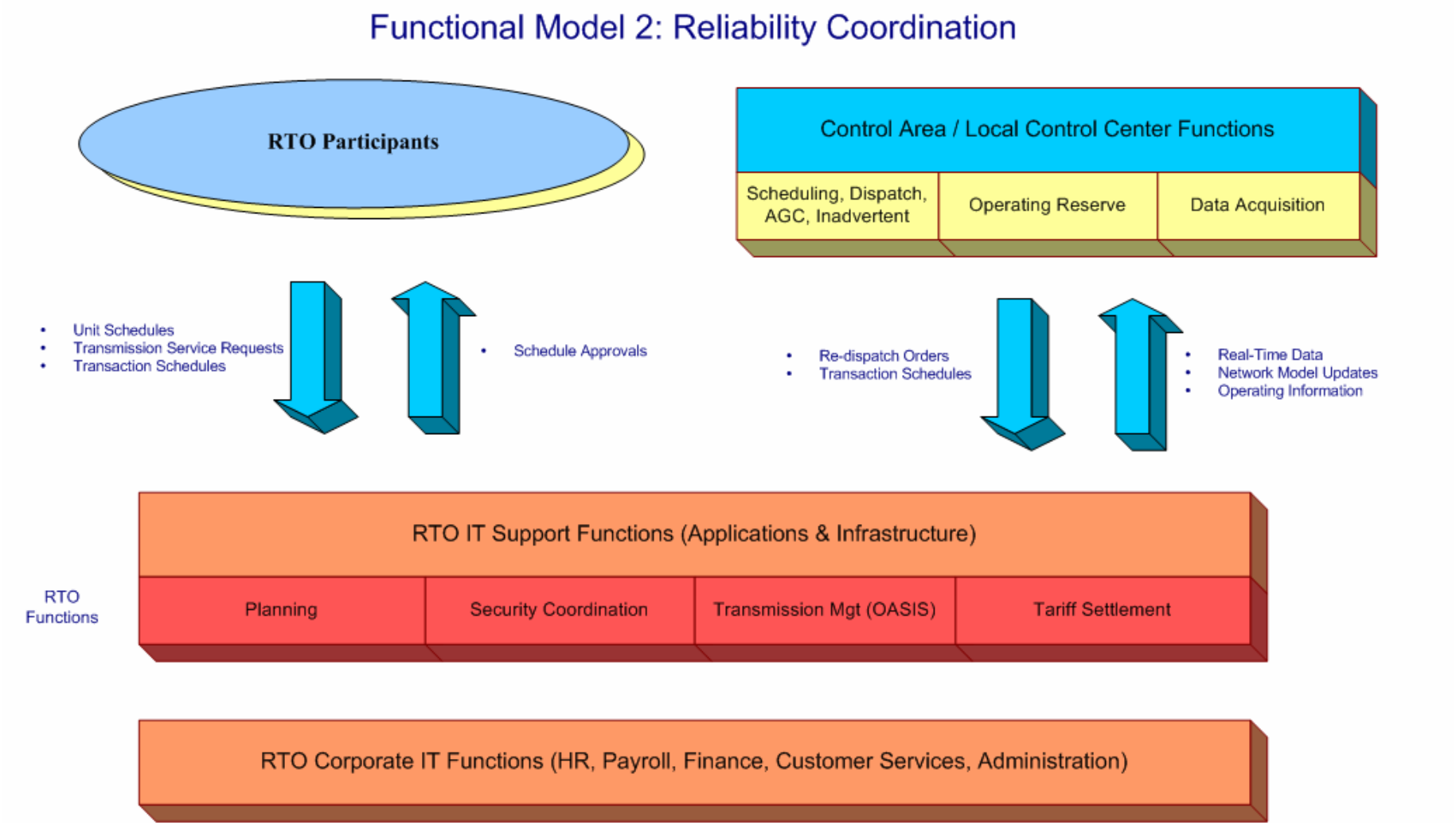
3. The following are critical focus areas that the DOE has issued for securing SCADA environments:

- Identify all connections to SCADA networks.
- Disconnect unnecessary connections to the SCADA network.
- Evaluate and strengthen the security of any remaining connections to the SCADA network.
- Harden SCADA networks by removing or disabling unnecessary services.
- Do not rely on proprietary protocols to protect your system.
- Implement the security features provided by device and system vendors.
- Establish strong controls over any medium that is used as a backdoor into the SCADA network.
- Implement internal and external intrusion detection systems and establish 24 hour-a-day incident monitoring.
- Perform technical audits of SCADA devices and networks, and any other connected networks, to identify security concerns.
- Conduct physical security surveys and assess all remote sites connected to the SCADA to evaluate their security network.
- Establish SCADA "Red Teams" to identify and evaluate possible attack scenarios.
- Clearly define cyber security roles, responsibilities, and authorities for managers, system administrators, and users.
- Document network architecture and identify systems that serve critical functions or contain sensitive information that require additional levels of protection.
- Establish a rigorous, ongoing risk management process.
- Establish a network protection strategy based on the principle of defense-in-depth.
- Clearly identify cyber security requirements.
- Establish effective configuration management processes.
- Conduct routine self assessments.
- Establish system backups and disaster recovery plans.
- Senior organizational leadership should establish expectations for cyber security performance and hold individuals accountable for their performance.
- Establish policies and conduct training to minimize the likelihood that organizational personnel will inadvertently disclose sensitive information regarding SCADA system design, operations, or security controls.

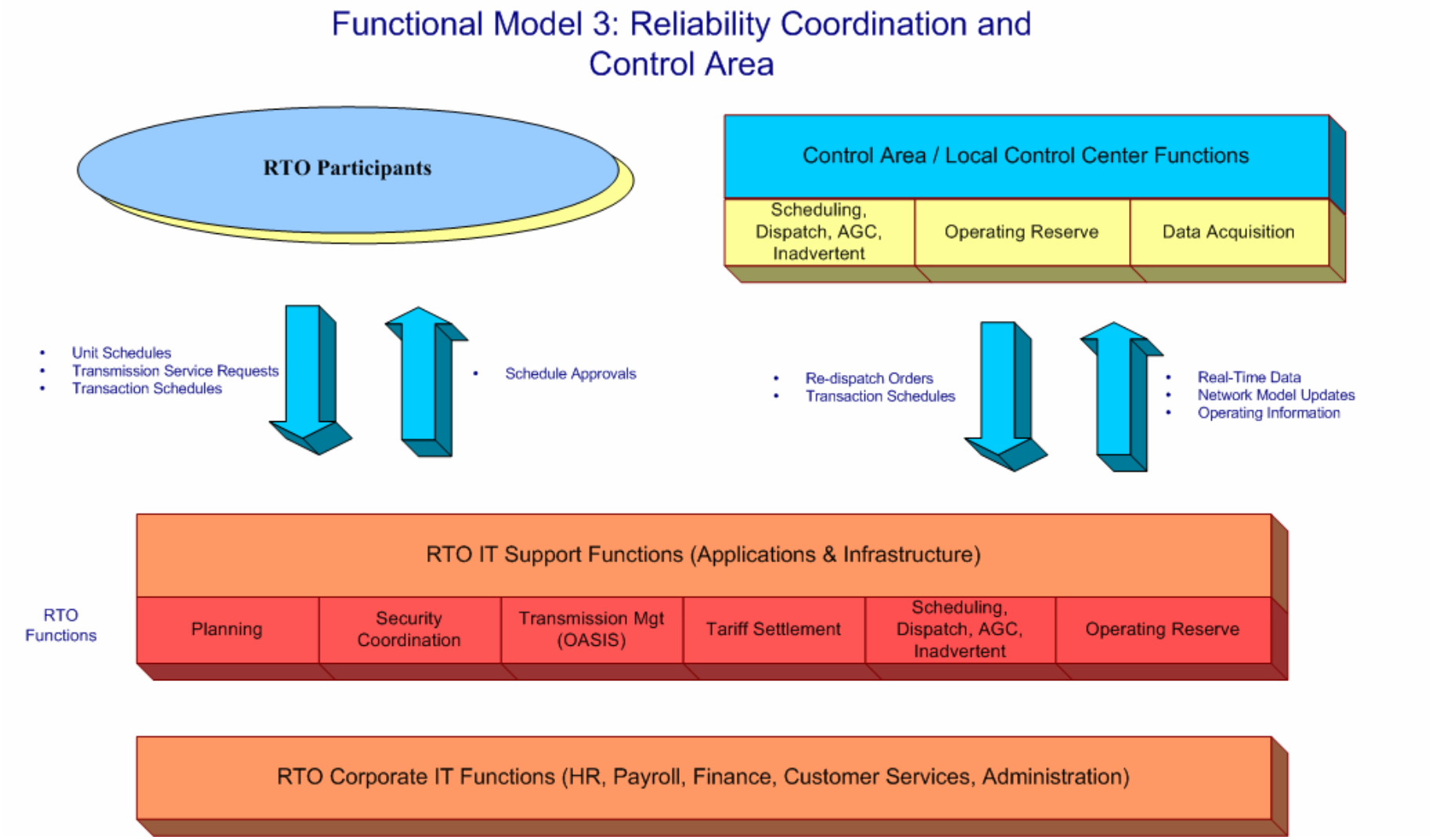
IX. Appendix C: Model 1 - Control Area



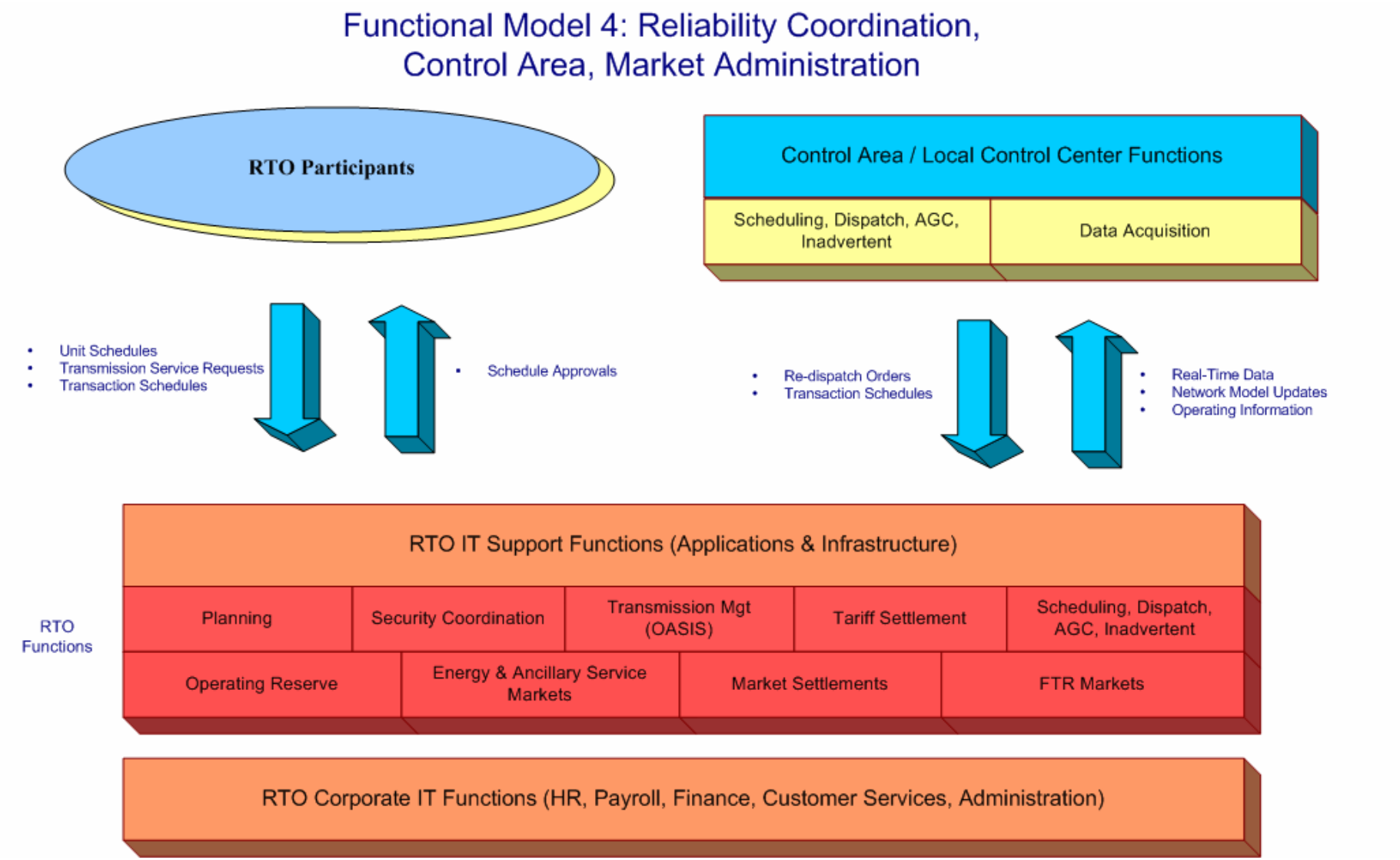
X. Appendix D: Model 2 - Reliability Coordination



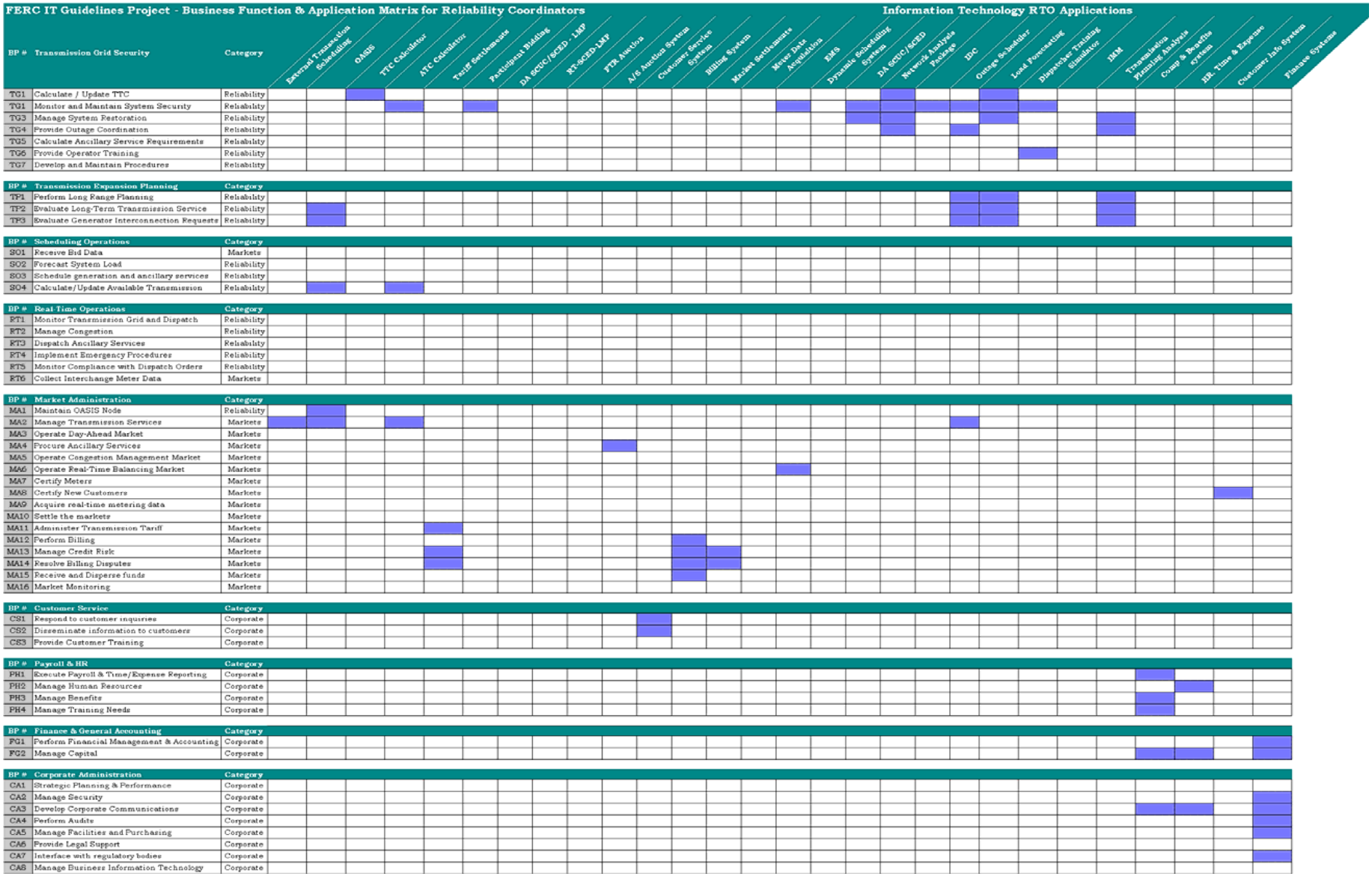
XI. Appendix E: Model 3 - Reliability Coordination and Control Area Functions



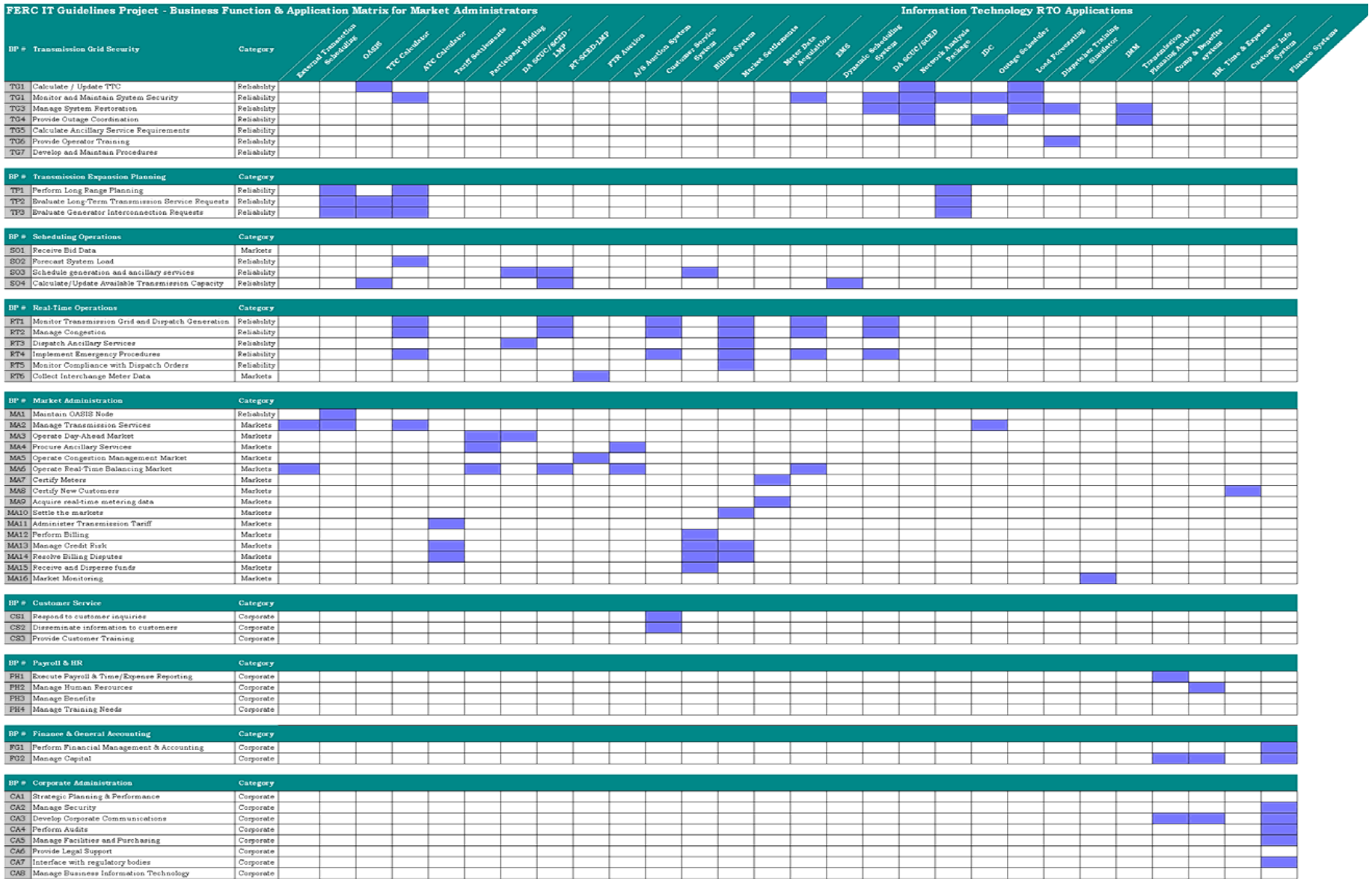
XII. Appendix F: Model 4 - Reliability Coordination, Control Area Functions and Market Administration



XIII. Appendix G: Business Applications – Reliability Coordinators



XIV. Appendix H: Business Applications – Market Administrators



XV. Appendix I: Business Function & Infrastructure Matrix

FERC IT Guidelines Project - Business Function & Infrastructure Matrix

Information Technology Infrastructure Elements

BP #	Transmission Grid Security	Category	Servers (OS)	Storage	Switches (LAN)	Routers (WAN)	RTU	Circuits	Network / Systems Mgt	NOC / Help Desk	Network Tools	Network Security	Desktops	PBX / Centrex / VoIP	Voicemail	Turret Consoles	Wireless LAN / Last Mile	Internet Connectivity	Remote Access	Disaster Recovery
TG1	Calculate / Update TTC	Reliability	P	P	P	P	P	S	S	S	P	P	S	S			S			P
TG2	Monitor and Maintain System Security	Reliability	P	P	P	P	P	S	S	S	P	P	S	S	P		S			P
TG3	Manage System Restoration	Reliability	P	P	P	P	P	S	S	S	P	P	S	S	P		S			P
TG4	Provide Outage Coordination	Reliability	P	P	P	P			S	S	P	P	S	S			S			
TG5	Calculate Ancillary Service	Reliability	P	P	P	P			S	S	P	P	S	S			S			
TG6	Provide Operator Training	Reliability	P	P	P	P			S	S	P	P	S	S			S			P
TG7	Develop and Maintain Procedures	Reliability	P	P	P	P			S	S	P	P	S	S			S			P
BP #	**Transmission Expansion Planning**	**Category**																		
TP1	Perform Long Range Planning	Reliability	P	P	P	P		P	P	P	S	P	S	S			S			
TP2	Evaluate Long-Term Transmission	Reliability	P	P	P	P		P	P	P	S	P	S	S			S			
TP3	Evaluate Generator Interconnection	Reliability	P	P	P	P		P	P	P	S	P	S	S			S			
BP #	**Scheduling Operations**	**Category**																		
SO1	Receive Bid Data	Markets	P	P	P	P			P	P	P	P	S	S			P			P
SO2	Forecast System Load	Reliability	P	P	P	P			S	S	P	P	S	S			S			P
SO3	Schedule generation and ancillary	Reliability	P	P	P	P		P	S	S	P	P	S	S	P		S			P
SO4	Calculate/Update Available	Reliability	P	P	P	P			S	S	P	P	S	S			S			P
BP #	**Real-Time Operations**	**Category**																		
RT1	Monitor Trans. Grid and Dispatch	Reliability	P	P	P	P	P	P	P	P	P	P	S	S	P		S			P
RT2	Manage Congestion	Reliability	P	P	P	P	P	P	P	P	P	P	S	S	P		S			P
RT3	Dispatch Ancillary Services	Reliability	P	P	P	P	P	P	P	P	P	P	S	S	P		S			P
RT4	Implement Emergency Procedures	Reliability	P	P	P	P	P	P	P	P	P	P	S	S	P		S			P
RT5	Monitor Compliance with Dispatch	Reliability	P	P	P	P	P	P	P	P	P	P	S	S	P		S			P
RT6	Collect Interchange Meter Data	Markets	P	P	P	P	P	P	P	P	P						P			P
BP #	**Market Administration**	**Category**																		
MA1	Maintain OASIS Node	Reliability	P	P	P	P		P	P	P	P	P	S	S			P			P
MA2	Manage Transmission Services	Markets	P	P	P	P		P	P	P	P	P	S	S			S			P
MA3	Operate Day-Ahead Market	Markets	P	P	P	P		P	P	P	P	P	S	S			S			P
MA4	Procure Ancillary Services	Markets	P	P	P	P		P	P	P	P	P	S	S			S			P
MA5	Operate Congestion Mgt Market	Markets	P	P	P	P		P	P	P	P	P	S	S			S			P
MA6	Operate Real-Time Balancing Market	Markets	P	P	P	P	P	P	P	P	P	P	S	S			S			P
MA7	Certify Meters	Markets	S	S	S	S			S	S	S	S	S	S			S			S
MA8	Certify New Customers	Markets	S	S	S	S			S	S	S	S	S	S			P			S
MA9	Acquire real-time metering data	Markets	P	S	P	P	P	P	P	P	P	P	S	S			S			S
MA10	Settle the markets	Markets	P	P	P	P		S	S	S	P	P	S	S			S			S
MA11	Administer Transmission Tariff	Markets	P	P	P	P		S	S	S	P	P	S	S			S			S
MA12	Perform Billing	Markets	P	P	P	P		S	S	S	P	P	S	S			S			S
MA13	Manage Credit Risk	Markets	S	P	S	S			S	S	P	S	S	S			S			S
MA14	Resolve Billing Disputes	Markets	P	P	P	P		S	S	S	P	P	S	S			S			S
MA15	Receive and Disperse funds	Markets	P	P	P	P		S	S	S	P	P	S	S			S			S
MA16	Market Monitoring	Markets	P	P	P	P		S	S	S	P	P	S	S			S			S
BP #	**Customer Service**	**Category**																		
CS1	Respond to customer inquiries	Corporate	S	S	S	S		S	S	S	S	S	S	S			P			S
CS2	Disseminate information to customers	Corporate	S	S	S	S		S	S	S	S	S	S	S			P			S
CS3	Provide Customer Training	Corporate	S	S	S	S		S	S	S	S	S	S	S			S			S
BP #	**Payroll & HR**	**Category**																		
PH1	Execute Payroll & Time/Expense	Corporate	P	S	P	P		S	S	S	P	P	P	S			P	P		P
PH2	Manage Human Resources	Corporate	P	S	P	P		S	S	S	P	P	P	S			P	P		P
PH3	Manage Benefits	Corporate	S	S	S	S		S	S	S	S	S	S	S			P	P		S
PH4	Manage Training Needs	Corporate	S	S	S	S		S	S	S	S	S	S	S			P	P		S
BP #	**Finance & General Accounting**	**Category**																		
FG1	Perform Financial Management &	Corporate	P	P	P	P		S	S	S	P	P	S	S			S			P
FG2	Manage Capital	Corporate	P	P	P	P		S	S	S	P	P	S	S			S			P
BP #	**Corporate Administration**	**Category**																		
CA1	Strategic Planning & Performance	Corporate	S	S	S	S		S	S	S	S	S	S	S			S	S		S
CA2	Manage Security	Corporate	P	P	P	P		P	P	P	P	P	P	S		S	P	P		P
CA3	Develop Corporate Communications	Corporate	S	S	S	S		S	S	S	S	S	S	S			S	S		S
CA4	Perform Audits	Corporate	S	S	S	S		S	S	S	S	S	S	S			S	S		S
CA5	Manage Facilities and Purchasing	Corporate	S	S	S	S		S	S	S	S	S	S	S			S	S		S
CA6	Provide Legal Support	Corporate	S	S	S	S		S	S	S	S	S	S	S			S	S		S
CA7	Interface with regulatory bodies	Corporate	S	S	S	S		S	S	S	S	S	S	S			S	S		S
CA8	Manage Business Information	Corporate	P	P	P	P		P	P	P	P	P	P	S		S	P	P		P

Key	
Primary	
Significant	
Modest	
Minor	
None	

XVI. Appendix J: Business Applications & Infrastructure Matrix