AN ITIL® ROADMAP:

DEVELOPING A SERVICE & PROCESS IMPROVEMENT PLAN

Version : 1
Date : November, 2004
Author : Troy DuMoulin
TABLE OF CONTENTS

1 ROADMAP ........................................................................................................................................ 3

2 PROCESS DEPENDENCIES .......................................................................................................... 5

   2.1 INCIDENT MANAGEMENT / SERVICE DESK ........................................................................... 6
   2.2 CHANGE MANAGEMENT ................................................................................................. 7
   2.3 PROBLEM MANAGEMENT ............................................................................................... 8
   2.4 SERVICE LEVEL MANAGEMENT ................................................................................ 8
   2.5 CONFIGURATION MANAGEMENT .............................................................................. 9
   2.6 RELEASE MANAGEMENT ............................................................................................ 10
   2.7 CAPACITY MANAGEMENT .......................................................................................... 11
   2.8 AVAILABILITY MANAGEMENT ................................................................................ 11
   2.9 IT SERVICE CONTINUITY MANAGEMENT ................................................................ 13
   2.10 FINANCIAL MANAGEMENT FOR IT .......................................................................... 13
   2.11 IT SECURITY MANAGEMENT ..................................................................................... 14
   2.12 COMPUTER OPERATIONS .......................................................................................... 15

3 SUMMARY ...................................................................................................................................... 17

4 ABOUT PINK ELEPHANT ............................................................................................................ 18
1 ROADMAP

One day Alice came to a fork in the road and saw a Cheshire cat in a tree. “Which road do I take?” she asked. “Where do you want to go?” was his response. “I don’t know,” Alice answered. “Then,” said the cat, “it doesn’t matter.”

Lewis Carroll

Unlike our heroine in the tale of Alice in Wonderland, this paper assumes that the reader has made a decision to implement or at least expressed an interest in the IT Infrastructure processes defined by ITIL. The natural result of having made this decision is the question, where do I start?

When developing a roadmap of where and how to start implementing the processes defined by ITIL, there are several considerations to take into account.

The approach is typically expressed by the following questions:
- Where are we now? (People, Process, Technology)
- Where do we want to be?
- How are we going to get there?

Based on these questions, an organization can use the following model to assist with the development of a customized roadmap of what processes they will implement in a sequential order.
1. The first task to accomplish is to establish a benchmark or baseline of process maturity by either doing a self-assessment or by having an external provider such as Pink Elephant provide a point in time reference. This activity provides necessary input into the decision making process as well as providing the added benefit of establishing a starting point, which can be referenced when expressing improvements that have been realized by the ITIL program.

2. The next step is to then plot each process on the grid pictured above to determine how each process can potentially affect the business from a risk perspective. The IT organization has the potential to greatly facilitate business goals. However, failures in IT controls and processes have the potential to also essentially disable business beyond recovery from a technical, legal, and reputation perspective. Example: An immature Release and Change Management process can impact an online trading system significantly.

3. The third axis of input should be guided by the consideration of a number of organizational issues, such as process dependencies, organizational culture, funding, resources, political ability to influence, the need to establish early quick wins, etc. Based on these three input axis, an organization can begin to establish a roadmap unique to their situation.

Based on this model, it should become clear where a specific organization would start and how a program focused on process improvement can then be defined. However, the one missing element in this model is the fact that processes have a sequential order of dependency based on input and outputs, which must be taken into consideration. Additionally, other factors such as level of difficulty and current IT culture must be taken into account. For example, from a pure logic perspective one might assume that Configuration Management should be implemented first since it plays a critical role in almost every other major IT process. The challenge with this philosophy is that it is also seen as one of the most difficult processes to implement successfully due to the factors listed above and does not have a chance if Change Management has not gained a reasonable level of control over the IT environment.

The following paper has been written to assist an organization in understanding the current state of the processes within their organization and to provide insights into major dependencies between processes.
2 PROCESS DEPENDENCIES

While several of the decision factors listed in this paper are unique to each organization, there is one consideration that based on general ITIL principles remains relatively static. Based on logic and sequence, certain processes need to be in place at a relatively mature state in order to support the introduction of others. For this reason “Process Dependencies” can be defined with all other things being considered equal.

To start the discussion, there are two basic premises to consider:

1. IT’s role is to support, control and manage defined IT Services for the business customer (Incident, Change and Service Level Management).
2. Certain processes are customer facing while others occur behind the scenes (Incident, Change, and Service Level Management).

With these two considerations, one starts to see that the same three processes begin to take on a logical sequence. Regardless of the other factors listed, most organizations will start with these three processes for the following reasons.

1. Support of IT Systems is a core and most visible element of Service delivery.
2. Uncontrolled and unplanned changes have an adverse effect on Service delivery.
3. IT is difficult to impossible to plan or become proactive unless IT has defined what Services it provides at what levels.

- What is not defined cannot be controlled and stabilized
- What is not controlled and stabilized cannot be measured consistently
- What is not measured consistently cannot be improved

Caveat: The following section will look at each process in relationship to typical levels of observed deployment within organizations. Maturity levels are indicative of normal evolution and are not necessarily representative of a Capability Maturity Model (CMM) perspective. Use the process descriptions in terms of understanding where your processes are currently in relationship to their effectiveness against the controlled state defined by ITIL.
2.1 Incident Management / Service Desk

The processes and functions related to supporting the business are a core element of the IT organization as well as a very visible process to the end user. Most organizations have a formal support function established with a process to fix things already in place at some level of maturity. Improvements in this process are relatively quick to obtain with high benefit to the business customer. The implementation of this process is typically seen as a quick win relative to other processes without requiring major organizational change. For these reasons, Incident Management is almost always a starting point for an ITIL implementation program. Examples of typical levels of implementation would look as follows:

1. A formal function is in place to receive user calls and register them in a call tracking software. There is no real distinction between incidents, service requests, and informational requests. Reporting accuracy is limited due to the inconsistent classification and update of records. At this level of maturity there are little to no process dependencies.

2. The next level of maturity is typically represented by the following description. In addition to having a formal function in place to receive user calls, a defined process has been established which documents how calls are received and classified in accordance with documented policies. Incidents, Service Requests and Informational Requests are registered as distinct process objects. Defined polices include:
   A. An agreed prioritization model considering impact and urgency
   B. An agreed assignment, escalation and notification model
   C. An agreed record classification structure, which includes a component, type, item classification as well as a closure code indicating a probable source of the incident.

3. A mature implementation of Incident Management includes the previous examples and is practiced consistently across all functional areas. The process is seen as an organizational activity as opposed to the job of the Service Desk. Incidents are registered from other areas that do not have a user impact, including computer operations and network management events. The Service Request process is seen as a type of change request and is dealt with in accordance to the policies defined under Change Management. The definition of “Significant Incident” and the trending of repeat incidents are done in support of Problem Management. Obvious dependencies for an Incident Management process at this level include Change and Problem Management.
2.2 Change Management

Change Management is a process, which by its lack of maturity can have the most dramatic impact on the business. Unapproved, unplanned, and uncoordinated changes can impact the business customer on a frequent basis. Additionally, without the ability to control when, how and by whom things are changed in the production environment, other processes such as Release and Configuration Management cannot be effectively implemented. A controlled Change Management process is a dependency for several other IT business practices. For this reason, Change is typically among the first processes organizations choose to implement. Approaches organizations take to implement this process follow a typical pattern:

1. Change Management at a very basic level of maturity is implemented in order to facilitate communication of when and how a set of changes will take place. The principle of the process at this level is simply to provide a heads up on what is being tossed over the production fence. Communication is largely done through email, and if there is a formal meeting to discuss the changes, the attendees are required to have a very pressing reason why a change should be delayed. Most changes at this level of maturity are passed through due to a lack of effective power. The process is seen mostly as a nuisance, which simply delays getting “real work done.”

2. The next level of Change Management is often referred to as Change Control. The basic premise of a process at this level of maturity is that all changes should be scheduled in accordance with each other and placed in what ITIL calls a forward schedule of changes. At this level of maturity, the process can drive compliance effectively and there is a lead-time policy that indicates how long in advance a change must be submitted, based on identified complexity and business risk. A formal meeting is typically held to discuss the change schedule with the primary purpose of approving the upcoming schedule as opposed to the changes themselves. Typical, problem areas with a process at this level of maturity are the handling of urgent or expedited changes. This level of maturity is required in order to support the processes of Configuration and Release Management.

3. The fully mature change process occurs earlier in the change lifecycle than what has been defined as Change Control. At this level of maturity, there is some defined mechanism for approving the conceptual fact that the change should actually occur as well as the coordination and scheduling element of the act of making the change in the production environment. At this level, large changes such as projects and application enhancements may be conceptually approved in what is perceived as a separate process; however, all changes regardless of functional area, size or complexity should be coordinated and scheduled by a single process.
2.3 Problem Management

Problem Management depends on an Incident process that has been established at a level of maturity, which produces consistent Incident classification and data for trending in support of problem identification. Once Incident Management can reliably produce this level of input, the data can be trusted to support the implementation of Problem Management. Approaches organizations take to implement this process follow a typical pattern:

1. The first activities the organizations implement that are traditionally associated with the Problem Management process is the “Major Incident Review” process, often referred to as a post-mortem activity. The premise of this activity is to review high impact incidents to determine root cause and implement measures to avoid a re-occurrence. This activity is often implemented under the management of the incident restoration process and is often led by a service desk team lead or manager.

2. The next level of maturity is the realization that Problem Management is a distinct process that requires its own process models, policies and resources and is supported by incident reporting and trending activities. While at this point the process is implemented at a level of maturity that has significant benefits, the majority of activity is still focused on reactive problem identification and elimination.

3. The third level of Problem Management implementation typically includes the identification or proactive issues for the explicit purpose of incident avoidance. An example of this is where the patch management process is understood to be part of the Problem Management process. When a vendor signals that a security vulnerability or deficiency has been found in their product, a Known Error record is opened for the purpose of impact analysis and assessment. If the Known Error is deemed to be applicable, then the Release and Change Management processes are engaged to validate, test, approve, and deploy the patch into the production environment. Obvious process dependencies include Release, Change and Configuration Management.

2.4 Service Level Management A

In order to implement additional processes from this point forward, it is critical to define the baseline of IT Services provided by the IT Organization. Contrary to popular belief and practice, the creation of Service Level Agreements (SLAs) is not the first step in the implementation of SLM. There are three progressive levels of implementation of Service Level Management, the first of which is a dependency for several other processes:

1. The definition of technical services and professional capabilities provided to the business.
2. The ability to monitor the IT organization’s capability to meet internal IT targets for service delivery.
3. The Development of a service provisioning agreement with the client called a Service Level Agreement. (Phase B)
Service Level Management B

Once IT Services have been defined and catalogued and the IT organization has developed the capability to consistently deliver and monitor those services, agreements can be developed and signed off with the customer. Many organizations will implement SLM in two distinct phases:

A. The first phase entails the development of a Service Catalog, which in essence describes a global SLA with the business organization as a whole.

B. The second phase entails the development of specific SLAs with individual customers or Lines of Business.

In order to support processes such as Configuration, Availability, Capacity, IT Service Continuity and Financial Management, IT Services and their default attributes and levels of provision need to be defined.

2.5 Configuration Management

The premise of Configuration Management is the identification and control of all configuration items (CIs) within the scope of the process. While identification can be achieved through the use of manual and automated means, the concept of control is dependant on a relatively mature Change Management process. Change Management drives compliance for Configuration Management and the scope of the two processes needs to be closely aligned.

Additionally, much like Service Level Management Configuration Management can be implemented at three levels:

1. Inventory Management is the management of stand-alone records describing objects and their attributes within the various IT environments.

2. Asset Management is the addition of financial attributes, which track the cost of owning and supporting the IT environments. These costs are allocated back to a costing and charging mechanism managed by Financial Management.

3. Configuration Management refers to the ability to track CIs at a relationship level. Relationships are modeled from both a technical as well as business usage and impact perspective. At a physical level, relationships such as application to server are managed. At business level, physical components are mapped to IT Services or Professional Capabilities, which are in turn mapped to the business customer in support of business impact analysis.

In order to map IT components to services and business customers, Configuration Management has a dependency on Service Level Management having defined services and their relationship to business consumers. (SLM A)
2.6 Release Management

The goal of Release Management is the assurance of quality, production readiness and deployment of any new or modified element being introduced to the live customer environment. To accomplish this, the Release Management process collects requirements from each stakeholder group and then matches those requirements to release types that are defined by an agreed risk impact model. Based on these release types, the appropriate number of requirements is applied in order to assure production readiness. It is the role of Release Management to broker which requirements apply for each type and at each milestone of the release lifecycle. The efficiency and effectiveness of the process is based on the right sizing of the number of requirements for each type based on business risk. The challenge of Release Management lies in the fact that there are numerous stakeholder groups that all have very strong views on the subject.

Typical stakeholder groups would include:
- Application Development
- Project Office
- Security Group
- Architectural Engineering
- Facilities / Cabling
- Computer Operations
- Production Support
- Quality Assurance functions
- Change Management process
- Configuration Management process
- Service Level Management process
- Etc.

1. A first level of maturity for this process typically places the quality assurance role in the hands of the Change Management process. Change advisory meetings are long and tedious due to the fact that questions have to be asked and requirements validated as to the quality and completeness of the proposed change request. At this level of maturity, there is a strong dependency on a change process at the level defined as Change Control.

2. The second level of implementation typically focuses only on the stakeholder groups, which are seen as the production support groups. A Release process at this stage of maturity is often called a “Production Handover Process”. Release requirements are only focused at the last milestones of the lifecycle which occur just prior to and during deployment into the production environment.

3. A fully mature Release process includes requirements for the full release lifecycle from all of the groups listed above. Release types are defined which have been allocated the appropriate set of requirements. These requirements are published and integrated into the application lifecycle as well as the project management methodologies. Change
Management at this point looks to Release to attest to the fact that all requirements have been met and that the appropriate sign-offs have been achieved.

While many processes integrate with the Release Management process, the primary relationships are Change and Configuration Management.

Note: The processes from this point forward can be implemented in any sequence due to the implementation of Service Level and Configuration Management.

2.7 Capacity Management

Capacity Management is a tactical process that manages capacity issues from a technical as well as service perspective. While certain elements of Capacity Management are not dependant on other processes, the more mature aspects of the process have explicit dependencies on processes such as Configuration and Service Level Management.

Capacity Management has three typical phases of implementation:

1. The first level of Capacity Management is the management of components and collections of components. An example of this level of implementation is the management and monitoring of individual and collections of servers from a resource and threshold perspective. Capacity Management at this point is executed as a departmental or functional responsibility.

2. The next level of Capacity Management is the roll up of individual components into a collection of objects, which facilitate an IT System such as Microsoft Exchange or SAP. This level of Capacity Management is dependant on Configuration Management having done the mapping of relationships on these systems.

3. The final level of Capacity Management is the proactive planning element, which considers the input of the monitoring aspects of the process as well as the tactical and strategic inputs received from the business in regards to future development needs. An annual plan is produced which considers future requirements in regards to capital projects, ongoing operations and new technology consideration. To be effective, a tight integration is required at this point with the Service Level and Financial Management processes.

2.8 Availability Management

Availability Management is a tactical process that has both a reactive monitoring and tactical planning aspect. The objective of the process is to facilitate the availability of the IT Services provided to the business customer in relationship to agreed times. Contrary to popular practice, this process has more activities than monitoring and reporting overall availability. Other key activities of the process include:
A. The coordination of inspective and proactive maintenance
B. The architectural engineering of IT Systems with availability requirements in mind
C. Close integration with IT Security Management
D. Close integration with Problem Management for error elimination
E. Close Integration with Configuration and Service Level Management

Like other processes, Availability Management has typical phases of implementation that require dependencies on other processes.

1. The first level of maturity typically results in availability of individual components or collections of components being tracked and reported back to the business customer. This usually results in the presentation of overall server availability and a list of incidents attributed to the users of a specific line of business. The dependencies at this level of maturity would be the use of systems monitoring tools and the reliability of the Incident Management data.

2. The next level of Availability Management is the roll up of individual components into a collection of objects, which facilitate an entire IT System such as Microsoft Exchange or SAP. This level of Availability Management is dependant on Configuration Management having done the mapping of relationships on these systems. Monitoring and reporting of availability is now done with a higher level of accuracy and granularity.

3. The ITIL activities of “Maintainability” and “Serviceability” refer to inspective and proactive maintenance scheduling with internal departments as well as external suppliers. While the internal element of this process has no other process dependencies, the external suppliers typically are managed by an underpinning contract. To successfully negotiate the changes related to Serviceability, this may require the intervention of Service Level Management.

4. The ITIL activity of “Resilience” refers the engineering of fault tolerance into a system design based on customer requirements. These requirements are typically gathered by the Service Level Management process and then scoped by an engineering function in alignment with policies defined by Security Management.

5. The final level of Availability Management is the proactive planning element, which considers the input of the monitoring aspects of the process as well as the tactical and strategic inputs received from the business in regards to future development needs. An annual plan is produced which considers future requirements in regards to capital projects, ongoing operations and new technology consideration. To be effective, a tight integration is required at this point with the Service Level, IT Service Continuity and Financial Management processes.
2.9 IT Service Continuity Management

The objective of the IT Service Continuity Management is to define requirements and then provide the business with the appropriate level of IT Service in the event of a crisis or disaster. As the name indicates, this process is dependant on those services being defined in Service Level Management and modeled within the Configuration Management Database (CMDB). That being said, this process, like the others, has various levels of typical implementation based on maturity. Dependencies on other processes become more critical as the process is defined at a more mature level.

1. The first level of maturity is typically represented by the disaster recovery requirements being defined and implemented by the application life cycle methodology when the system first goes live. CI attributes and relationships are defined and used to setup the disaster recovery (DR) capability as a one-time activity. Further updates to the DR capability and documentation are typically done periodically as a point in time ‘catch up’ project. At this level of maturity, the absence of the other processes is mitigated by explicit project activities as a single occurrence. The risk with this approach is that changes to the system, which can potentially happen on a frequent basis, are not reflected in the DR capability and recovery documentation. This level of maturity represents a significant risk to an organization, which is depending on the process at this level of maturity to actually support the defined DR requirements. The one dependency that is important at this level is integration with Incident Management. A policy has to be defined, which describes when and how an Incident breaches a tolerance level and becomes a crisis requiring the enactment of the DR plan.

2. The next level of maturity recognizes the dependency and reliability of the DR capability, and documentation relies on integration with Change and Configuration Management.

3. The subsequent phase of implementation is when the organization realizes that IT Service Continuity is an ongoing process instead of an element of a project lifecycle. Requirements are gathered from the business in relationship to risk tolerance and DR requirements. These requirements are then fed into processes such as Service Level, Financial, Availability and Capacity Management for sizing and costing activities. Based on annual testing, results are fed back to the business and improvement activities are brought back into the process.

2.10 Financial Management for IT

The primary activities of Financial Management include costing, accounting and potentially charge back of costs to the client. Most organizations have a rudimentary costing and budgeting process based on a technical instead of service mindset. This is largely due to the missing input of other processes such as Service Level and Configuration Management. In principle, the services defined in the Service Catalog are the same services that are modeled within the CMDB. These same service definitions should represent the general ledger accounts and chargeable...
elements that appear on a client bill. Without this integration, the Financial Management process is typically implemented along the following levels of maturity.

1. Costing models are targeted at understanding the cost of individual or like collections of assets or resources, such as an individual server or collection of servers. Costs for these technical components or people resources are bundled and allocated back to the business customer based on a shared allocation model not representative of actual use. Forecasts and actual expenses are based on a technical model. If services are defined, they are done so from a financial perspective that is not representative of the actual services delivered to the business by the IT organization. At this point of maturity, there are no real dependencies as the Financial Management process mitigates the lack of other processes by defining costs models and chargeback systems at a best effort level.

2. As indicated above, the services defined in the IT Service Catalog should form the basis for the budget model and the GL accounts defined in the costing, reporting and forecasting models. This level of maturity requires Service Level Management to be implemented at least to the point that services are defined. In order to establish which costs are direct and indirect, Configuration Management is required to establish the relationships between components as they relate to IT systems and services.

3. At its most mature level, Financial Management requires trusted input from the following processes in order to determine annual budgets and approve proposed annual capital and operational expenditures:
   - Service Level Management
   - Availability Management
   - Capacity Management
   - IT Service Continuity

2.11 IT Security Management

The process of Security Management is required to establish the necessary logical and physical security measures to ensure (Confidentiality, Integrity and Availability) C.I.A. of IT Systems and information. This process is typically implemented at various phases of maturity:

1. The first level of maturity is concerned with the definition of security policies, which are enacted on technical devices and components such as firewalls, user permissions, data access, etc. For detailed guidance on defining these technical policies, organizations refer to best practice models such as the ISO security standard 17799. At this level of Security Management, there is a recognition that a policy and procedure has to be defined on how to handle specific security related incidents. As indicated in the Roadmap graphic at the start of this session, the implementation of logical and physical security typically is done prior to the pursuit of other ITIL processes.

© Pink Elephant, 2004. The contents of this document are protected by copyright and cannot be reproduced in any manner.
2. The next level of maturity recognizes that Security Management is a repeatable process as defined in ITIL, which has explicit and ongoing integration dependencies with multiple processes. The primary relationships include:

- Change Management
- Configuration Management
- Service Level Management
- Availability Management
- IT Service Continuity Management

2.12 Computer Operations

As a process, Computer Operations is primarily concerned with the monitoring and scheduling of IT System events, such as batch and Storage Management activities.

1. At its basic level, computer operations need to be aware of how and when jobs that interrupt the provisioning of IT Services to clients can occur. This information requires a level of understanding of availability windows and online transaction timeframes. If formal processes for Service Level and Availability Management have not been defined, these timeframes are typically agreed to by the clients based on requirements that have been defined around the system based on the initial project managed by the application lifecycle methodology.
2. At a more mature state, Computer Operations has an explicit integration with the following processes:

- Change Management
- Service Level Management
- Capacity Management
- Availability Management
- IT Service Continuity Management
3 SUMMARY

In summary, the sequence of processes listed in this paper is an attempt to take a logical and pragmatic look at which processes need to be implemented in what order based on dependencies. While this order makes sense when all things are considered equal, sadly they rarely are. The reader should use this paper as an input into the decision making process based on the unique situation of their organization.

"Two roads diverged in a wood and I – I took the one less traveled by."

Robert Frost
4 ABOUT PINK ELEPHANT

Pink Elephant is the world leader in IT management best practices, offering conference, education and consulting services to public and private businesses globally, and many listed in the Fortune 500. The company specializes in improving the quality of IT services through the application of recognized best practice frameworks, including the Information Technology Infrastructure Library (ITIL®).

Service Lines

Pink Elephant’s service lines each provide different, but complementary business solutions:

- **Business Process Consulting**: Using the ITIL best practices approach to IT service management as a springboard, Pink Elephant provides end-to-end solutions – from assessments, to strategic planning to implementation, continuous improvement and beyond. Experienced consultants work hand-in-hand with customers every step of the way.
- **Conferences & Special Events**: Pink Elephant is the world’s largest producer of IT service management conferences and delivers several major events per year.
- **Education**: Pink Elephant is the most prolific creator and widespread distributor of ITIL training, delivering three levels of certification – Foundation, Practitioner and Management. Pink Elephant is accredited by The Examination Institute for Information Science (EXIN) and The Information System Examination Board (ISEB).
- **PinkATLAS™**: PinkATLAS™ is a secure, web-enabled knowledge management system containing much of Pink’s highly valued intellectual property – ready and waiting for users to access, copy, customize and re-use.

ITIL Leadership

Pink Elephant has grown to become recognized globally as The ITIL Experts and is very proud of its commitment to the ITIL best practice framework. In fact, Pink Elephant has been involved in the “ITIL project” since its inception in 1987, and was recently selected by the UK’s Office of Government Commerce (OGC) to help author ITIL’s next version. Furthermore, Pink Elephant:

- Supported the development of ITIL’s core books:
  - Service Support (English and French editions)
  - Service Delivery
- Launched PinkVerify™, the only independent certification program worldwide that recognizes software that supports specific IT management processes.
- Created the International IT Service Management Conference & Exhibition, one of the largest events worldwide solely dedicated to ITIL.
- Facilitated plans for EXIN’s North American examination centre (Loyalist College in Belleville, Ontario, Canada), enabling a faster and easier ITIL certification process.
- Introduced ITIL internationally to companies across a wide variety of industries, sizes, technical platforms and corporate cultures.
• First offered the Foundation, Practitioner and Management ITIL certification levels publicly in North America
• Was a founding member of the IT Service Management Forum (now itSMF) – the worldwide networking group for IT service management professionals

To learn more about Pink Elephant’s services visit www.pinkelephant.com, or call us at 1-888-273-PINK.

Awards

Pink Elephant is recognized as a progressive and successful company and is the recipient of the following awards that reflect its corporate leadership excellence and business results:

• Top 100 Woman Entrepreneurs – 2001 – 2006: Awarded to Pink Elephant CEO, Fatima Cabral, by PROFIT magazine
• Ontario Global Traders Award – 2005: Awarded by the Ontario Government for achievements in innovation, leadership, product excellence and expansion into new markets
• Business Excellence Award – Awarded by the Federation of Portuguese-Canadian Business and Professionals to Pink Elephant CEO, Fatima Cabral
• Top 100 Fastest Growing Companies in Canada – Awarded annually by PROFIT Magazine. Pink Elephant was recognized as one of Canada’s fastest-growing companies (based on a comparison of revenue growth for five consecutive years)
• Top 100 Canadian IT Professional Services Organizations – Awarded by Branham300
• EXIN Award: Given to the organization with outstanding achievements in promoting the IT Service Management framework outlined in the IT Infrastructure Library (ITIL) – the world’s most popular set of IT management best practices

To learn more about Pink Elephant’s services visit www.pinkelephant.com, or call us at 1-888-273-PINK.