The Framework to Realign IT with the Business:
A Role of Data Protection

ZELJKO PANIAN

The Graduate School for Economics and Business

University of Zagreb

J.F. Kennedy Sq. 6

CROATIA

http://www.informatika.efzg.hr/zpanian

Abstract: - Availability, performance, and rapid recovery from unplanned outages are seen as principal goals to be achieved in contemporary information systems. But, it is often claimed that many IT departments are not providing an adequate level of service to the rest of the company. This has an impact on the way they are perceived, reducing their credibility and eliminating their place at the level where strategic decisions are made. Out thesis is that data protection plays a key role in achieving credibility of IT department, hence providing quality of service in backup/recovery field can be a strong proof of IT department's efforts to align their operation to most important corporate or business goals. The five-step framework is presented that may help IT organizations to achieve service excellence in their data protection efforts. It is also meant to be used as springboard to reinforce IT's renewed alignment with the needs of the business. In effect, this framework is a model of the best practices and approaches to improve data protection we have witnessed in operation in some of the best Croatian firms.

Key-Words: - Data protection, backup, recovery, business goals, service level management, service level agreement, quality of service

1 Introduction

Today, many IT teams are plagued relentlessly by complex issues that keep them in constant fire-fighting mode of behavior. They use precious staff resources to correct ongoing availability or restore problems that are highly visible to the organization, yet relatively unimportant in the larger scope of managing IT systems. In the face of IT challenges like exponential data quantity growth, outsourcing, server farming and consolidation, flattened budgets, and company reorganizations, IT managers and their staff are on the defense and under the pressure to simply ensure basic services delivery.

Availability, performance, and rapid recovery from unplanned outages are seen as principal goals to be achieved. According to some recent surveys of customer satisfaction, the ability of an IT organization to meet these three goals directly impacts how favorably a company's executives and leadership perceive IT [1].

It is often claimed that many IT departments are not providing an adequate level of service to the rest of the company. This has an impact on the way they are perceived, reducing their credibility and eliminating their place at the level where strategic decisions are made [2].

IT infrastructures have also become increasingly complex, with corporate acquisitions adding to the problems of managing disparate assets spread across the globe. Most enterprise infrastructures have become a patchwork of heterogeneous components – systems and software based on wide variety of platforms, operating systems, and vendors. Backup shortages and allowable downtime are becoming virtually nonexistent because business is conducted on the 24/7 basis and all around the world [3].

Thus, IT professionals have good reasons to be concerned. Research from an industry analyst firm confirms that IT's worst fears about its ability to recover critical data in the event of an emergency [4]. According to the same source, as much as 60 percent of all backups performed in today's network environments are not completed successfully.

2 Turning Defense into Offense: A Customer-centric Paradigm

More than ever, IT departments are being forced to account for new projects and demonstrate tangible results of their ongoing investments in infrastructure and processes [5]. Yet in the face of these mounting challenges, the emergence of a new

breed of IT manager can be seen – individuals who actively move beyond the fire fighting mode of behavior, regaining control and leading their organization to support their company's evolving corporate strategies. Rising to the challenge, these leaders are proactively embracing opportunities to reshape their company's perceptions of the IT organization.

By borrowing key concepts from external service providers, IT leaders view the success of their IT organization from a customer-centric paradigm, redefining IT success based on two types of criteria [6]:

- The quality and value of the services they offer
- How well their IT services align with the current and future business objectives of their customers.

To meet these criteria, data protection visibility and connecting data protection efforts to larger IT initiatives should be achieved.

2.1 Data Protection Visibility
As a part of forward-thinking efforts, IT leaders are using a simple, but undervalued IT function to gain visibility across the enterprise, and to demonstrate their organization's effectiveness at meeting business needs. This opportunity for IT to redefine itself centers on the hidden "backroom" data protection and recovery efforts already underway across the enterprise. Namely, data protection efforts present a rare opportunity for IT to demonstrate excellence and tight alignment with business goals [7].

Later in the paper, we will outline five simple steps to help ensure IT organization's performance aligns with the needs of the business itself. We have developed this multi-step framework based on the best practices we have seen in several IT groups in Croatia. These are the organizations that have been able to successfully migrate from defense to offense, from reacting to the latest fires to proactively planning and managing operations, allowing them to forecast resources more effectively.

Interestingly, the steps in this simple framework do more than demonstrate IT's alignment with business goals. Organizations following these steps achieve significant improvements in their data recoverability rates. They minimize their operating costs and achieve amazing improvements in the utilization and

efficiency of their existing IT assets and staff, and prove performance against compliance objectives while improving communications.

2.2 Connecting Data Protection Efforts to Larger IT Initiatives
Before exploring the five-steps framework, it is important to describe a few of the initiatives IT organizations use to measure their success in data protection and recovery. These initiatives include:

- The Capability Maturity Model (CMM), as applied to an organization's backup and recovery efforts
- Key aspects of Service-Level Management (SLM), including the concept of Service Level Agreements (SLAs)
- Renewed emphasis on customer-centric communication.

2.2.1 Capability Maturity Model
Capability Maturity Model (CMM) has been originally developed by Software Engineering Institute and designed to ensure that software products are developed to high standards. But, the model's tenets have since been applied to many other areas of IT.

The CMM structure outline is presented in Table 1.

Level	Maturity	Sampling of Key Indicators
5	Linked	Recovery strategy aligned with data value
4	Optimized	Quality charts, efficiency management
3	Proactive	LAN free backups, restore testing, operations policies and procedures
2	Reactive	Backups impact LAN services, multiple point solutions, success/failure reporting
1	Unmanaged	Failing backups, no documentation

Table 1 – The CMM structure [8]

The model describes five levels of organizations maturity. Organizations residing at the lowest levels (1 or 2) tend to react more to events and incorporate little process or documentation in their efforts. As the organization moves to higher levels (3, 4 or 5), there is more proactive behavior, more control of current

processes, more communication both within the group and to the group's customers, and a better connection between the IT group's efforts and the goals of the business.

2.2.2 Service-Level Management and Service Level Agreements

One of the best ways today's IT leaders have found to ensure that an enterprise recognizes and values IT's strategic importance is by demonstrating how closely IT aligns its own efforts with the specific needs and goals of the business. Service-Level Management (SLM) defines a successful IT organization as offering a set of IT services that are inextricably linked to the goals and processes of the business [9].

In backup/restore procedures, there are IT leaders at the forefront of SLM that define their success by how well they are meeting predefined backup/restore service levels or qualities of service (QoS). Such predefined service levels form the basis of either informal or formalized Service Level Agreements (SLAs) made by both IT management and key company leaders who hold a vested interest in the data and systems under IT domain.

The five-step framework proposed is based on strong SLM principles. Using the framework, IT organizations can logically progress, step-by-step, through the process of identifying core service level expectations of IT customers, determining how best to position IT to deliver expected service levels, and ways to validate, publicize, and improve on IT performance against service level goals. This framework also prescribes key SLA criteria, external benchmarks and best practices currently in use by some of today's top Croatian IT groups to measure the success of their data protection activities.

2.2.3 Customer-centric Communication

We believe there is one fundamental difference that separates IT organizations that succeed at business realignment from those that fail: communication. Successful IT organizations consistently reinforce and recognize customer-centric communication as the core of service excellence. Whether they follow tenets of the CMM or SLM, these organizations make it a priority to communicate goals, objectives, status, and progress toward better aligning themselves with customer needs.

As IT organizations progress toward better alignment and higher levels of maturity, their communication matures to providing validation and ongoing confirmation that IT is aware of data protection expectations, and is actively working to meet or exceed objectives. The initial discussions with the key IT customers and executives should cover expectations about how IT will communicate progress, success or failure at meeting objectives. Commitment toward both inward- and outward-facing communication plays an integral role in IT's success at reshaping and defining the image it presents to customers as proactive, progressive and closely aligned.

3 The Five-Step Framework to Realign IT with the Business

The five-step framework is designed to help IT organizations to achieve service excellence in their data protection efforts. It is also meant to be used to reinforce IT's renewed alignment with the needs of the business. In effect, this framework is a model of the best practices and approaches to improve data protection we have witnessed in operation in some of the best Croatian firms.

These IT organizations rose above an ongoing fire fighting approach and defensive posture as they responded to pressing backup and restore issues. They successfully transformed themselves into proactive, customer-facing groups who actively provide robust data protection services to a host of IT customers and who seek to meet or even exceed customer expectations with their quality of service.

The steps included are:

1. Assess state of service delivery
2. Align SLAs with business goals
3. Identify areas for improvement
4. Remedy performance gaps
5. Prove performance

The five key steps in this framework are depicted on Fig. 1.

3.1 Assess State of Service Delivery

Each improvement must begin with an understanding of the current levels and qualities of services delivered. To obtain enough information to effectively establish and benchmark organization's current levels of backup/restore services, appropriate reporting tools should allow:

- Understanding backup success trends over time.
- Drilling down to a very granular level of reporting on specific backup success and failures, or getting higher-level summary reports on backup success levels.
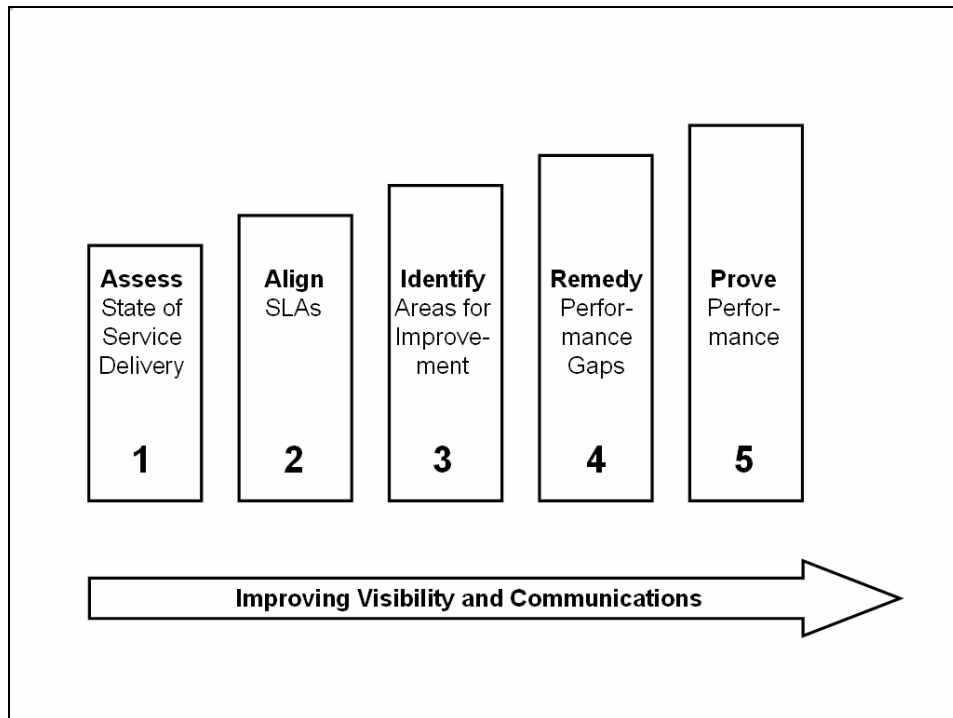
Fig. 1 – Five-Step Framework to Realign IT with Business Needs

- Identifying the success or failure of backups performed for key data owners or groups, backups associated with specific protection jobs, and backups executed on specific directories, servers or clients.
- Specifying different classes of data and identify backup success or failure for each. According to F. Moore, one suggested way to categorize data is as follows: mission-critical, vital, sensitive or non-critical [10].
- Identifying common categories of backup errors that may be causing bottlenecks at either the file level, at the tape drive, somewhere else in the network or within the backup software application itself.
- Identifying specific servers or files that have been inadvertently omitted from backup process.
- Locating the backup jobs or data owners that tend to consume the most backup resources over time.
- Learning how backup operations and user behavior are changing over time.
- Learning how current backup-related assets are being used across the enterprise, such as typical utilization rates on all of the organization's tape libraries and other backup media.

3.2 Align Service Level Agreements with Business Goals

The second step in the framework is a fact-finding mission conducted by IT. During this step, IT conducts interviews with all key customers and gathers data on industry standards for system performance and cost of service. There are three good reasons for this second step:

- Demonstrate IT's renewed, customer-centric focus. This can serve as an excellent public relations campaign because it demonstrates that IT management is open and interested in learning about the specific needs and goals of different leaders in the business and how these goals relate to customer expectations for accessing, protecting and restoring their application data.
- Document specific customer service needs. The outcome of this fact-finding mission should be a set of working documents that define the customers' criteria and expectations of IT services for backing up and restoring their data.
- Establish definitive benchmarks to define success. Beyond receiving input from customers, this step also allows IT to establish its own backup/restore success

criteria based on the best practices and common service level measurements taken from other industry sources.

3.3 Identify Areas for Improvement

In effect, this step is the reality check that allows the organization to understand the gaps in their IT performance, based on the assessment conducted in Step 1 and desired service levels identified in Step 2. The gap can exist between:

- The current quality of service offered in backup/restores; and,
- The desired quality of service that should be offered.

This step also leads to understanding if services are delivered at the lowest possible cost.

The organization can consequently optimize the delivery of backup/restore services by offering QoS levels to customers at the lowest cost to the company [11]. One obvious opportunity to do this will come in terms of improving on how the organization utilizes current backup-related assets and hardware.

This step also involves assessing backup trend data, and any reports related to the current utilization of backup resources. It is opportunistic and requires IT to search constantly for ways to work smarter and improve processes and resource usage. IT managers must actively seek new ways to cut or contain operating costs and consolidate performance, while driving higher standards of availability, performance, recoverability or utilization.

3.4 Remedy Performance Gaps

Step 4 is one of the most critical steps in the framework presented. By acting upon the knowledge gained in previous steps, the organization can prioritize and fix backup/restore issues identified during the analysis of their environment.

Based on the priorities set, the organization can now actively troubleshoot and remedy chronic sources of backup errors. The company will also need to correct any glaring bottlenecks to backup/restore performance. If certain levels of backup or restore are identified that current systems cannot achieve, there is a need to start modifying systems to satisfy customer resource requirements. In some cases, this may involve acquiring new systems or software to deliver required levels of service.

At the end of this step, IT organization should have instituted a set of regular reports for internal/external customers. For example, reports can be automatically posted to a internal Web portal, accessible at any time by the key data owners and customers in the company. Or, in other case, reports on the ongoing backup/restore performance related to the customer data can be automatically send via e-mail. In either case, these reports serve to communicate and remind data owners of IT success at delivering quality services to meet the needs of the business.

3.5 Prove Performance

The final step in our framework is the "prove it" step. This is where IT organizations really have a chance to publicize their efforts to align themselves with the needs of the business. Validating performance at this step means offering independent reports about how successful IT organization is at achieving the SLA criteria set for their internal or external customers. Ongoing, automated reports easily demonstrate how well the organization is doing at complying with all of the predefined SLA criteria.

If IT organization has achieved significant gains in performance or has been able to significantly lower cost of operations, this is also where they can publicize their progress to customers, executives and upper level management. This helps raise confidence levels in IT's ability to contain costs and operate efficiently.

4 Iteration

IT organizations dedicated to ongoing growth in data protection should recognize that completing only one five-step framework will not ensure continued progress. The framework presented is not intended as a linear progression with one starting and one ending point, but as an iterative, ongoing process. As soon as an IT organization completes the last step in this framework, they should start planning to begin the whole process again.

IT organizations truly set themselves apart from their peers when they consistently assess where they are, work with customers to identify where they need to be, and are actively doing all that is possible to close performance gaps [12]. These organizations are constantly seeking ways to optimize their service delivery and gain best possible use of existing resources.

By repeating these five steps, today's IT organizations continue to transform themselves

from tactical to strategic, from a position of reaction to one of anticipative leadership. This emphasis on continuous process improvement will succeed in continuing to raise the bar for IT excellence in today's organizations.

5 Conclusion

Organizations that follow the basic steps outlined in the framework presented will be able to produce respectable results in a relatively short period. Those that drive their data protection efforts from a reactive, fire-fighting mode of behavior into proactive planning and capacity utilization initiatives can focus on delivering quality service at lowest possible cost. In the process, these IT groups transform their image within the company. Where once they may have been considered s significant cost center and just another department, many of these IT groups have reshaped their image to one of a quality service provider, offering the best services to customers at the lowest possible cost.

Based on key concepts in the most progressive IT management initiatives, this five-step framework has proven itself time and again as a means to demonstrate an IT organization's ability to understand and meet larger goals of the business.

The steps in this framework help IT move away from reaction – and limited visibility on current backup successes or failures – toward proactively communicating backup/restore performance, reporting on quality of service performance against service level agreement criteria, documenting overall backup policies, and discovering how to improve asset utilization and forecast future growth needs.

Within just a few months of implementing this framework we believe any IT organization can achieve similar success at realigning its data protection/recovery efforts to meet the needs of the business.

The end result will be an IT organization that understands and meets customer needs and the larger initiatives of the business. Such an IT group will be able to proactively communicate on an ongoing basis with customers about progress as well as issues related to their application data.

References:
[1] ***. "Service-Level Management – Best Practices". http://www.nextsim.org/bestprac_slm.html, 01/2005
[2] Donaghue, A. "Utility computing: Just because you can, should you?". http://comment.zdnet.co.uk/andrewdonaghue/, 01/2005
[3] Janssen, M., Verbraeck, A. "The added value of e-intermediary business models", Proceedings of the Infonomics/Merit Workshop on Digitalisation of Commerce, Maastricht (Netherlands), 10/2001, pp. 86-100
[4] Biggar, H. "IT's Dirty Little Secret". InfoStor Zine, http://is.pennet.com/Articles/, 11/2004
[5] Vitt, E. Luckevic, M., Misner, S. *Making Better Business Intelligence Decisions Faster*. Microsoft Press, Redmond (Wa), 2002.
[6] Clabby, J. *Web Services Explained: Solutions and Applications for the Real World*. Prentice Hall PTR, Upper Saddle River (NJ), 2003
[7] Goodwin, Ph. "Proactive Data Protection: The Best Defense Is a Good Defense". http://www.metagroup.com, 04/2004
[8] ***. "Capability Maturity Model". http://www.sei.org, 1998
[9] Hagel, J. "Managing for Business Results: Harnessing the Power of IT Management Systems". http://www.agilebrain.com/hagel.html, 04/2003
[10] Moore, F. "Storage and Security Report". NewsFactor's Data-Storage Today, http://data-storage-today.newsfactor.com, 05/2004
[11] Panian, Z. "What Does the Term 'E-Service' Really Imply and Mean?". 4th International Conference on Electronic Commerce, Hong Kong (China), 10/2002., Proceedings on CD
[12] Lientz, B. P., Rea, K. P. *Dynamic E-Business Implementation Management*. Academic Press, San Diego (CA), 2001.