



# Successful SLAs:

## *Step by Step*



---

September 2005



# Table of Contents

- Introduction ..... 3
- Service Level Agreements (SLA)..... 3
- The Key to SLAs: Making Data Protection Measurable ..... 5
- Step One: Assess the Data Protection Environment..... 5
- Step Two: Align the Degree of Protection with Business Goals..... 6
- Step Three: Identify the Specific Terms of the SLA ..... 7
- Step Four: Remedy Service Shortfalls..... 8
- Step Five: Prove Performance ..... 8
- Summary and Conclusion ..... 9
- About Bocada..... 9

## Introduction

Data protection activities are typically seen as operational, rather than strategic to the business. Proving business value has been difficult because the focus has always been on the procedures of “backup” rather than the broader goal: to ensure the continued availability and ongoing retention of extremely valuable and vital corporate assets.

When there is uncertainty about whether data is truly protected – a strategic business concern – the typical remedy is simply to run more backups. When IT departments operate in this reactive mode, the perception is that data protection is an operational “black hole.” The company throws in money with no certainty or visibility into the outcome or return on investment. And like a black hole, the data protection activities themselves are invisible. The IT department only gains recognition when something breaks – a server fails, and then missed or failed backups result in irrecoverable data. Bringing focus only on the failures results in a negative, skewed and undeserved perception of the IT department, and is a situation that is all too common.

### **SLAs in Action: Case Study**

#### ***Enterprise Profiled***

- Fortune 100 software company

#### ***Business Imperative***

- Verify that critical data is protected

#### ***Key Elements of SLA***

- Ensure that backups are scheduled and executed in accordance with daily change requests from data owners
- Capture information 24x7 and detect failures at all times
- Achieve overall success rate of 98%

#### ***Result***

- Goal of 98% success rate met for 12 consecutive quarters

## Service Level Agreements (SLAs)

Service Level Agreements (SLAs) are gaining traction as a way for proactive IT departments to demonstrate and prove the value of their data protection services.

SLAs are essential parts of the contract when enterprises outsource data protection to third-party providers. But more and more, in-house data protection teams are discovering that implementing SLAs for their internal customers is an extraordinarily effective way to not only prove the value of their services, but drive down the cost to the company by matching service cost to data value.

A well-crafted SLA assists all parties:

**The service provider or IT organization**, by specifically defining customer expectations and levels of service. For contracted providers, it also stipulates penalties and/or payment for inadequate service, or bonuses when goals are exceeded.

**The client or data owner**, by furnishing complete knowledge of the services to be delivered, and guarantees of performance backed by specific penalties.

**The CIO**, who can implement specific standards and practices for data protection squarely focused on business objectives, and demonstrate to business managers the capabilities and limitations of IT systems in meeting those goals.

**The executive team**, which gains an understanding of the true risk of lost data to the enterprise, and the cost of lowering that risk.

Whether it is an internal agreement or a third-party contract, a data protection SLA delineates specific expectations of service. A standard SLA generally details these areas:

- Client objectives (known as Service Level Objectives, or SLOs) and how a provider promises to meet them
- Specific service(s) to be provided and levels of delivery
- Detailed methodology of delivery
- Delivery performance metrics such as reports of backup successes and failures, restores performed or tapes archived
- Responsibility for delivery measurement and reporting
- Reporting methodology and frequency
- Methods and level of provider responsiveness
- Expectations for future add-ons to the SLA
- Fees to be charged for services delivered
- Client responsibilities and duties
- Penalties for non-delivery or under-delivery of services

## SLAs in Action: Case Study

### ***Enterprise Profiled***

- Fortune 500 medical technology company

### ***Business Imperative***

- Share management view that summarizes success rates and prove the IT department is meeting objectives against Sarbanes-Oxley policy requirements

### ***Key Element of SLA***

- Achieve and prove a success rate of 95%

### ***Result***

- Performance records stored and reported to management with ease through an automated reporting application that generates out-of-the-box SLA and restore reports

## The Key to SLAs: Making Data Protection Measurable

To create an SLA and then prove its requirements are being met, there must be some way to objectively measure and verify performance.

It is possible to quantify data protection activities manually by reviewing log files and individual backup application reports, interpreting the results and coming up with some measure of backup successes and failures. Some IT departments go this route, but the SLAs are necessarily limited in scope and require inordinate amounts of staff time to verify. In addition, especially for third-party contractors, there is some skepticism of the results, given that the organization responsible for meeting the SLA is also creating the reports.

An automated reporting application is the key to developing and implementing SLAs. In addition to supporting the metrics required, such an application should also be:

- **Multi-vendor and vendor-neutral.** Capable of generating reports in heterogeneous backup environments, accommodating the full range of backup applications, platforms and devices.
- **Focused on data protection rather than backup.** Support a wide range of metrics that go beyond operational reports of individual backup successes and failures. It should report on the data protection status of individual servers, clusters of servers by department, and report on global parameters of interest to data owners including GB/TB protected and cost of services provided.
- **Third-party independent.** Free of any biases, or the appearance of them, by being from an independent vendor, and requiring no intermediate data manipulation by IT staff in order to generate reports.
- **Easy to install, use and maintain.** Minimally impact the computing environment; add few or no change-management burdens; and automate information-gathering and dissemination of reports to not burden the IT staff with additional duties.

With such a reporting tool, it is possible to implement SLAs with a proven, methodical step-by-step process that allows organizations to improve their data protection services and prove their value.

## Step One: Assess the Data Protection Environment

The first step toward developing a data protection SLA is gaining a clear view into the existing data protection environment, process and efficacy. A reporting application with the ability to look across the heterogeneous backup environment and consolidate reports of activity into a common format provides this view and helps establish baseline metrics. Otherwise, the goals would likely be unrealistic. "Make sure 100% of our data is recoverable, immediately, to any point in time, forever" might be desirable to the data owner, but extremely expensive for the business.

This initial evaluation is often an eye-opener. Most operations contain unseen backup failures resulting from defective media, network collisions, server glitches and inevitable human error. These neglected and failed backups are often chronic, and remain undetected and therefore uncorrected until circumstances demand a restore or an audit.

Typically enterprises that have installed a reporting application have found at least one server or database completely overlooked – and often containing business-critical information. And less-important resources are often found to be receiving daily full backups and a degree of protection far out of proportion to their value. A customer database obviously warrants a higher priority for backup than, say, an internal office-supply spreadsheet. A company can waste hundreds of thousands of dollars on needless backups of largely static data by putting those stores on the same schedule as the CRM system.

## SLAs in Action: Case Study

### **Enterprise Profiled**

- Fortune 100 energy company

### **Business Imperative**

- Meet the management directive for achieving policy compliance

### **Key Elements of SLA**

- Meet or exceed success rate of 95%
- Prove adherence to tightly defined schedules for both full and incremental backups, and specific retention periods for each

### **Result**

- Management relies heavily on automated SLA reports to verify that policy compliance standards are being met, and to review trends for improving performance

## Step Two: Align the Degree of Protection with Business Goals

Once current performance levels are known, IT management can work with the data owners and business units to arrive at appropriate levels of protection, based on the business criticality and time-sensitivity of each data resource. This includes anticipating the need for immediate recovery, the degree to which recovering aged data is acceptable and the need for data retention for archival purposes. Data which must be reproducible for compliance with government regulations calls for special scrutiny.

The key elements involved are:

- **In case of failure, how recent must the backup be?** In the case of contact management in a business where leads have especially high value, it might be an hour. For other applications, daily, weekly or even quarterly might suffice.
- **How quickly must the data be restored?** If faster restores are vital, more frequent full backups (vs. incremental backups) might be required.
- **What are archival requirements?** Some data owners may want to archive and maintain a monthly or yearly backup. Some data must be retained to protect the company in the event of a regulatory audit; some requirements call for data retention periods of up to seven years.

## Step Three: Identify the Specific Terms of the SLA

Given the degree of protection required, the IT department can arrive at a backup process and procedure which achieves it. It then turns those requirements into specific terms under which the measured services should be delivered.

The terms of the SLA should include:

**Metrics.** A variety of parameters can be used to measure and verify compliance. The SLA will include these measures and specify levels of acceptable performance. Ideally, the reporting application directly outputs these measures. Some useful ones for developing an SLA might include:

*Backup frequency.* The frequency of both full and incremental backups.

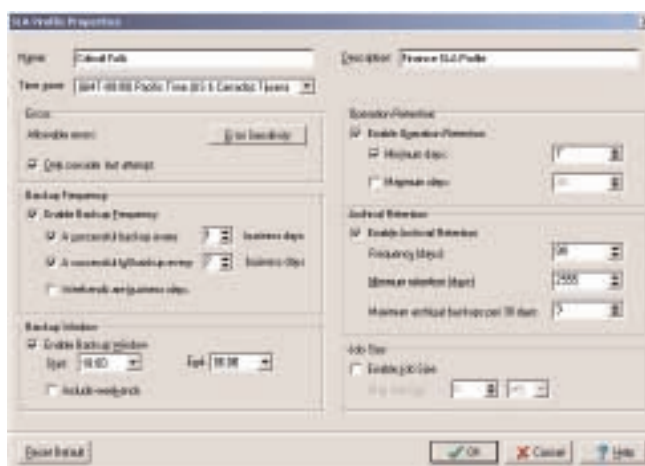
*Allowable errors.* The number of allowable backup errors, delineating a failed or successful backup. A reporting application should have an adjustable threshold, so that the “informational” or “notice” warnings output by some backup applications are not flagged as serious errors.

*Operational retention.* The length of time backup sets should be held in an easily accessible location, for performing restores.

*Archival retention.* The length of time legacy archives should be retained, for regulatory compliance, future audits or general business protection.

*Backup window.* The time during which the backup may run.

*Job size.* The total number of bytes backed up during each job.



A reporting application that directly tracks appropriate metrics makes it possible to create and track progress against SLAs without cumbersome manual reporting.

**Reporting requirements.** Ideally, the reporting application automatically pushes regular reports and proof of performance to the data owners via e-mail or posting to a web server. This eliminates any taint of possible data manipulation or other “cleansing” of the reports. For creating ad hoc reports, the system should allow direct querying of the database and generate reports automatically so administrators don't have to handle or manipulate the data. This eliminates questions about the integrity of the reports, and can be especially important in an audit situation.

**Event response.** If a backup fails or a restore is needed, the response requirement is normally instantaneous. In other cases, a 24-hour response window to remedy the failure or perform the restore may be adequate.

**Penalties.** An SLA without penalties is toothless -- it isn't really an SLA because there is no guarantee or incentive for success nor punishment for failure. Penalties may not be appropriate for a fully in-house operation, but should be standard for outsourced data protection services. A common SLA penalty is a month of service provider's fees waived for a failed restore, but when such a penalty is invoked, the data is already lost. A good recommendation is a combination of incentives and penalties.

For example, if *all* backups are completed, verified and retrievable in a given month, the service provider receives a bonus. For every failed backup that is irretrievable, there is a penalty. And, in the case of more than a pre-set number of failed backups in a set time period, penalties escalate.

**Costs.** Of course, pricing is an essential element of any contract with an outside provider. But even if an SLA is between a company and its internal IT department, costs can be made a part of the agreement.

Using market forces to drive data protection has proven incredibly efficient and effective for enterprises that have adopted the strategy. A charge-back system spreads costs among data owners — the more data they require to be protected or the more frequent their backup requirements, the larger amount of resources consumed and the larger their share of the costs. Typically, data owners’ requirements drop once they see the costs of “over protected” data hitting their bottom line.

Owner	Client	Files	Backups	Backup	GBs	GB	Total
Distribution	All clients	46,618	44	\$0.00	2.83	\$1.30	\$17.47
Engineering	All clients	18,064,875	8,363	\$0.00	6,517.54	\$1.30	\$19,861.63
Finance	All clients	11,564,323	5,071	\$0.00	2,561.73	\$2.60	\$12,837.73
Marketing	All clients	15,582,708	8,816	\$0.00	5,864.44	\$2.60	\$23,896.22
Operations	All clients	2,281,868	1,971	\$0.00	351.69	\$1.30	\$2,449.30
<b>Totals:</b>		<b>47,443,417</b>	<b>24,965</b>		<b>15,217.51</b>		<b>156,802.24</b>

Reporting the true cost of data protection to the business units allows chargeback, tying the degree of data protection to data value.

## Step Four: Remedy Service Shortfalls

The reporting application should clearly flag data resources that are at risk through unmet goals and borderline SLA performance, and that call for the highest-priority response. Ideally, it goes a step further by revealing the root causes of shortfalls, whether equipment failures, tape failures, faulty network cables, file-open errors or simple human errors such as failing to load the tape library.

Clearly showing failures and marginally protected data allows backup administrators to focus their troubleshooting efforts on the most critical assets.

Without this reporting, backup administrators spend much of their time focusing on isolated failures and sifting through log files, looking for clues to the causes. By contrast, the SLA, since it is driven by business value, brings the IT staff’s priority and focus to the failures that are truly business critical.

## Step Five: Prove Performance

An SLA, especially when combined with a reporting application that does cost accounting, can do much to elevate the perceived value of data protection efforts. Rather than providing a service to which the organization is essentially blind, the IT department is able to prove they are protecting critical business resources, by presenting empirical evidence in a readily accessible, frequently updated format.

Master Server	SLA Compliance %	Out-of-Comp
eserve.hardis.vorcorp.com	77	Errors, Size, Too Recent Full Backup, Retention
autl.virgl.vorcorp.com	73	Errors, Size, No Recent Full Backup, Too Early/Too Late, Retention
eng.virgl.vorcorp.com	71	Errors, Size, Retention
netbackup.virgl.vorcorp.com	70	Errors, Retention
sales.virgl.vorcorp.com	71	Errors, Size, No Recent Full Backup, Too Early/Too Late, Retention
tes.souflo.vorcorp.com	68	Errors, Size, No Recent Full Backup, Too Early/Too Late, Retention
tes.virgl.vorcorp.com	77	No Recent Full Backup, Retention

By viewing measures of performance against the SLA goals, the backup team can act to avoid contracted penalties – and more important, ensure that the data is protected.

The result is a strategic business intelligence approach that delivers an entirely different view of data protection. It becomes possible to graphically illustrate which areas are the most crucial, which are being neglected, and which are over-consuming resources. The company gains visibility into its use of storage media, hardware resources such as networks as backup servers, and the personnel that monitor and maintain it. It can then allocate those resources based on the value of the data.

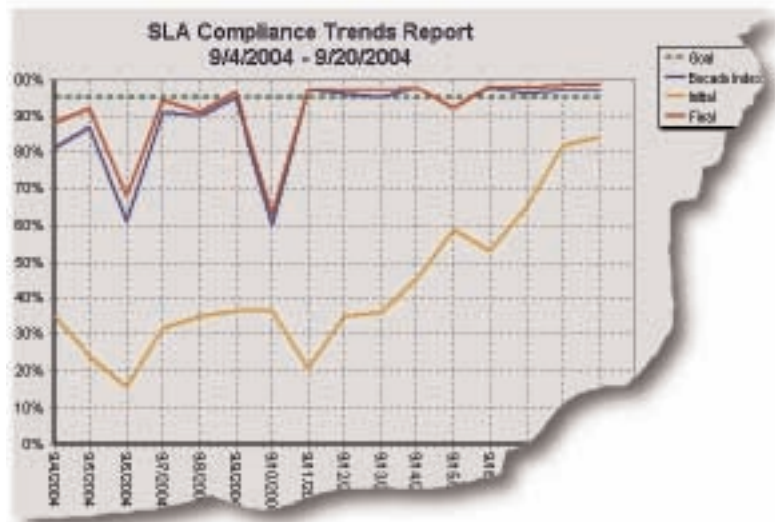
This allows backup administrators to move out of a reactive mode and into proactive management. Time previously spent gathering data on data protection activities, compiling reports manually and doing laborious detective work can be spent fine-tuning the systems for greater cost-effectiveness, matching resources to business needs, and continuously improving performance as measured against the SLAs.

## Summary and Conclusion

SLAs are a best-practices approach to data protection, and a strategic way for service providers and internal teams to prove the value of their services. Through a well-crafted SLA, data protection teams can move from a reactive stance where their services are largely invisible, to a proactive stance, with specific promises and regularly communicated proof of delivery.

## About Bocada®

Bocada is dedicated to ensuring that data protection services, systems and processes meet organizational objectives for quality, cost and compliance. Our flagship product, BackupReport®, provides objective insight into SLA performance, helping companies to improve data recoverability, reduce the cost of managing data protection operations, ensure compliance and communicate results. Bocada solutions have been deployed in more than 180 market-leading customer and partner environments worldwide, including Amgen, BankOne, Cap Gemini Ernst & Young, SBC Sprint, Unilever and Xerox. Bocada is a private company headquartered in Bellevue, Washington.



*By showing progress against SLAs, the IT department can not only prove compliance, but demonstrate the increasing value of its services.*



10500 N.E. 8th Street, Bellevue, WA 98004

Tel: (425) 818-4400 | Fax: (425) 818-4455 | [sales@bocada.com](mailto:sales@bocada.com) | [www.bocada.com](http://www.bocada.com)

---