

AUXIS™



Making IT Work: The Discipline

Getting IT "Under Control" to Enable Business
Effective Technology

By, Eric Liebross and Alvaro Prieto

2008

Introduction

Standards of have existed since human beings first evolved from apes. Most of these standards were established in response to environmental and cultural changes that required some level of measurement and control. Historical examples of the evolution of standards range from the Bible's documented guidance for Noah to determine the size of the Ark ("cubits"), to the Egyptian 365 day calendar, to the adoption of the metric system in 1793 by the French government.

The first recorded introduction of numbers in human communication occurred approximately 5,000 years ago, but even before that, historical artifacts survive that detail systems which tracked and oversaw articles of trade. Over time, a formalized approach to managing assets evolved, and in the 1400's today's modern accounting principles were developed and documented. Luca Pacioli, a renowned mathematician and a contemporary of Leonardo da Vinci, is called "the Father of Accounting" for his treatise on bookkeeping, "*De Computis et Scripturis*" ("*Of Reckoning and Writings*").

Today's Accounting follows the same basic principles laid out by Pacioli over 500 years ago, and it has evolved into a complex set of processes, standards and controls. GAAP ("Generally Accepted Accounting Principles") as dictated by the Financial Accounting Standard Board ("FASB") is used to govern the operations of businesses, governments and financial institutions in the United States, and most countries have similar sets of accounting rules.

It is impossible to imagine the conduct of business, indeed life, today without these standards being in place. However, one of the most fundamental and prevailing components of 21st century life, Information Technology ("IT"), has very few generally recognized and adopted standards. This situation is true across all sized businesses, but seems endemic in the middle market.

Mid market business executives, who would not dream of operating outside the rules of GAAP, are largely unfamiliar with the basic tenets of IT Standards and Control frameworks such as ITIL or CobiT, and more alarming, neither are their IT leaders.

IT Standards and Controls is not a "techie thing." In today's business world, where technology is completely embedded into business operations, it is integral to the successful operation of the business. IT Standards and Controls have direct impacts on business performance, profitability and customer service. A poorly controlled and disciplined IT operating environment can bring a business to a halt. A well controlled and disciplined IT operating environment can facilitate business performance, provide competitive advantages, and increase business profitability.

IT Standards and Controls: A Historical Context

Why are IT Operating Standards and Controls so poorly understood and adopted? Well, consider that the profession of Accounting has over 500 years of formalized history and adoption, and the process of accounting is thousands of years in the making.

Information Technology? The field was first introduced to business approximately 50 years ago, and arguably was not mainstreamed into business until 25 years ago. Adding to its “newness” is the fact that technology has evolved so rapidly, providing increased processing power, broader business application and greater span of control on an almost daily basis. Anyone old enough to remember the room-filling mainframe computers still marvel over the power and capability of a PDA.

So it’s no surprise that Information Technology is not as well controlled and managed as the field of Finance and Accounting. GAAP was initially developed at a time when the abacus was “state of the art” technology.

Clearly, Information Technology is not as mature a field as Accounting. But does that imply that the field must be “the Wild West”? Absolutely not. IT can and should be run in a disciplined, controlled manner. Its role in supporting day to day business operations, not to mention the high level of capital investment required to establish and maintain technology operations, necessitate that IT should be well controlled and aligned with the business.

Letting IT run without proper oversight, management and control is akin to letting the “tail wag the dog”. The key is in not letting technology govern IT operations, but in letting IT operations govern technology. But first, there must be the establishment of IT operating policies, controls and standards. Do these standards exist? Absolutely, but they must be adopted into the culture and

operations of the business in a realistic, practical way. And they must be actually followed, as well as measured and managed.

While all businesses follow GAAP, many organizations adapt GAAP principles to the “real world” operations of their businesses. Even external auditors have learned to accept “grey areas” in business accounting practices. IT Standards and Controls frameworks, like ITIL and CobiT, define IT operating principles, but their “real world” deployment must fit into the actual practices and performance of the business.

So what are these frameworks, and how should they be adopted into your business? First, let’s understand the dynamics of well run and poorly run IT operations, and their impact to the business. We call these dynamics of IT operations, “IT Discipline”.

Characteristics of a Poorly Disciplined IT Operation

Describing a poorly disciplined IT operation is reminiscent of Supreme Court Justice Potter Stewart’s definition of pornography: “I shall not today attempt further to define the kinds of material... but I know it when I see it.”

There are many characteristics of a poorly disciplined IT operation. It takes on many forms, insidiously affecting business operations in many ways, some obvious, some less so.

Reactive Support and Services

In an undisciplined IT operation, services are highly reactive. "Fire fighting" is the primary mode of operation, as IT spends a large amount of its time dealing with unplanned issues, outages and other "emergencies".

In this scenario, IT is often made aware of issues as they are impacting the business. Whether these impacts result from system outages, poor performance, security breaches or lost data, IT is often "the last to know", and is scrambling to fix the problem.

According to the IT Process Institute (ITPI), poor performing IT organizations spend more than 50 percent of their time on unplanned work activities¹, putting them in an almost constant "firefighting" mode. Microsoft recently conducted a survey that revealed that, on average, 30 percent of an IT Manager's time is spent on "firefighting".² The impact of this is that IT staff is being pulled away from business enabling activities, with less than 50 percent of the time available on planned or strategic work, and IT Managers are being distracted from focusing on strategically supporting business objectives. Put another way, if your organization's finance and accounting staff were spending a large percentage of its time tracking lost revenue, you would surely ask the question, "Why is the revenue being lost in the first place?"

So why is the business so accepting of IT failures and performance issues? Is IT reactivity a "necessary evil", or is it preventable? The ITPI goes on to say that high performing IT organizations spend less than 10 percent of the time "firefighting". If

this is true, then there are obviously ways to improve IT performance and control. Is the true IT "hero" the person who is constantly fixing problems that occur, or is it the person who prevents problems from happening in the first place?

Consistent System Performance and Downtime Issues

Another characteristic of the undisciplined IT operation is consistent system performance and downtime issues. While the level of infrastructure investments made by the business, the availability of hardware redundancy and the occurrence of uncontrollable events such as hurricanes and power outages play a large factor in performance and availability issues, well controlled IT operations is another important element in the equation.

In information technology, availability refers to the overall "uptime" of the system. Different businesses have different standards for availability, or "uptime".

For example, military defense systems require 99.9999 percent uptime, resulting in seconds of downtime during the course of a year. Financial services business, health care organizations, and large scale telecommunications organizations require 99.999 percent uptime, resulting in minutes of downtime during the course of a year.

The typical business operation may require a broader range of uptime requirements, typically ranging from 99 percent (days of downtime per year) to 99.99 percent uptime (hours of downtime per year.) The answer is a function of return on investment, as the way to achieve higher uptime is through

increased levels of technology investment, combined with strong operational controls.

A poorly disciplined IT operation does not align its “uptime” requirements with business performance and demands. Sometimes this actually results in over-investment, as the technology capital expenditure does not match the level of impact to the business from system outages.

The IT industry uses the term “high availability” to describe systems and technologies specially-engineered for high availability and reliability. These systems typically include redundant hardware and intelligent software designed to manage system failovers and transitioning. However, the cost in achieving high availability can be significant, so matching investment to business impact is a critical part of designing and managing IT infrastructure.

Another characteristic of poorly disciplined IT operations when it comes to system performance and availability are multiple single points of failure in the existing infrastructure. System uptime is not just a function of servers being online. The breakdown of a peripheral device, such as a router, switch or firewall, with no redundancy, can bring a network down as fast as a server failure. Single points of failure are essentially, “outages waiting to happen”. In poorly disciplined IT environments, these single points of failure often exist because the business is not aware of or understanding of the risks.

Some operational issues that impact system performance and availability include disaster recovery planning, business

continuity planning and change control. Disaster recovery planning and business continuity planning, two terms that are often over-used by vendors and IT professionals alike, are related to the preparation for events that cause system outages or performance issues.

Given the state of events in recent years, with the memories of 9/11 and Hurricanes Katrina and Wilma still fresh in the minds of business executives, more and more businesses have established some level of disaster recovery and business continuity planning. Even poorly disciplined IT operations have documented disaster recovery plans. However, have these plans been tested and updated over time? Have appropriate communication and deployment protocols been established? Has the impact on business operations been fully assessed and planned for? Too often, in the poorly disciplined IT operations, the answers to these questions are, “No.”, and the business does not realize it until it is too late.

Further, today’s technology requires constant upgrading and change to maintain currency and competitive advantage. Often, these changes are planned, but are not properly managed. Managing change is one of the most difficult challenges facing IT organizations, as IT infrastructure can potentially impact every part of the business operation. For example, a change in a router setting can impact anything from voice communications to email, to system availability to security. Any or all of these impacts can have an effect on business performance and profitability.

Effective change management means that not only are the changes planned for, the ways in which technology devices interact with business users, and the impact to these users due to system unavailability are understood.

In the poorly disciplined IT operation, change = problems. Business impact is not assessed, and risks are not understood and planned for. Change is poorly communicated, often resulting in unprepared users and poorly performed transitions. Worse, change is done "in a vacuum", undocumented, and even the entire IT Department may not be fully aware of what changes are taking place, making "cleaning up the mess" a difficult task.

As a result, a main characteristic of a poorly disciplined IT operation is the perception of system issues, even when they don't exist. Fear of technology change seeps into the business "subconscious", and IT is perceived as a business obstacle, rather than an enabler.

Poor IT Service Levels and Lack of Accountability

In the poorly disciplined IT environment, there are no clearly defined service levels for IT. Many businesses have not even defined, or are aware of appropriate measures for IT operations. So, IT continues to operate "on the fringe", without measurements of its performance, and with no clear audit trail to determine accountability.

Often, this is due to poor communication between the business and IT. The "IT guys"

are the "geeks" and "techies", unable to effectively engage with business users and executives. And unfortunately, sometimes, that's just the way IT likes it.

How realistic and practical is it to have a key part of your business disengaged from the rest of the enterprise? Would it be acceptable if the CFO could or would not report on the company's financial performance? Yet IT, which requires significant capital expenditure as well as ongoing recurring costs, is often not held to the same standard.

The issue is typically that IT standards and objectives are poorly defined and understood by the business. And even when these goals are defined, they are generally not well documented and measured. The result is inconsistent IT performance, and the inability to identify root causes to issues and quickly implement corrective measures.

Other symptoms of poor IT service levels and lack of accountability include costly project delays and failures, audit failures and higher than necessary audit and remediation expenses, poor visibility over IT activities and expenditures, unexpected expenses for IT infrastructure and services, and difficulties in supporting business changes that require technology implementation. The impact of this can be felt by the business in many ways, including reduced profitability, competitive disadvantages, customer service issues and margin erosion.

This lack of IT service levels and accountability is often "accepted" by the business, either due to limited understanding and/or involvement from the business with IT

or poor communication and/or openness from IT to the business. In many cases, it's a combination of both. And none of it should be acceptable.

Cultural and Organizational "Dysfunction"

The poorly disciplined IT organization is often "disconnected" from the rest of the business. It operates in a silo, sometimes even separated within itself. In IT, several "domains" may exist, including the network, server, desktop, telecommunications and applications areas. Many times these domains operate independently from each other, even though each is highly dependent upon the other. Effective cross-domain communication, inside and outside of IT, is a major challenge in an undisciplined IT environment.

This can be due to the lack of visibility over IT operations, and the barriers, both cultural and organizational, that are in place. The most significant factor in creating organizational "dysfunction" around IT is the company's culture.

"Cultural dysfunction" encompasses many factors, including politics, knowledge and experience, business objectives, rewards and incentives, management style, communication, pressures and other organizational dynamics.

Effective processes and controls can improve communication and resolve many of the cultural inhibitors that detract from IT operational performance. However, in the poorly disciplined IT environment, these processes are missing or ineffective, increasing the cultural and organizational

separation of IT from the rest of the business.

Other cultural and organizational characteristics of poorly disciplined IT environments include:

- Overly complex technologies with poor integration
- Poor IT leadership and lack of alignment with business leadership
- Limited process awareness or acceptance
- High levels of IT staff turnover
- Tightly controlled IT visibility and poor communication with the business
- Poor IT cost controls and budgetary overages; or conversely, under-investing in IT due to a lack of a clear value proposition

Characteristics Of A Well Disciplined IT Operation

Whereas a poorly disciplined IT operation can have many negative impacts on an organization, often, a characteristic of a well disciplined IT operation is that "nothing happens."

While somewhat "tongue in cheek", this definition is typical of the negative light that the business often views IT. IT is not recognized for its business enablement and support, instead only "seen and heard" when something goes wrong: systems go down, emails are "lost", the Internet is "slow", etc.

In the well disciplined IT operation, these events are rarities. In the well disciplined IT environment:

- Systems availability is within the range of the established targets, which are communicated and well understood by the business.
- IT tasks are more focused on strategic and planned activities, and “firefighting” is at a minimum.
- Change is effectively managed and communicated, and the introduction of new technologies is not viewed with trepidation.
- IT processes and controls are defined, documented and followed.
- These processes increase business performance, rather than encumbering it.
- IT is open and engaged with the business, and the organization is capable of attracting and retaining top level IT talent.
- IT has its “seat” at the “business table”, and investment in new technologies and IT operations is viewed as part of the overall business strategy.

In the well disciplined IT environment, IT is “seen and heard” for its accomplishments and business enabling value, and not viewed as a “necessary evil”.

Many factors come into play in establishing a well disciplined IT operation, but it is often rooted in the adoption of effective standards and controls, which establish a framework of “best practices” by which the business operates. There are many business

drivers for the use of IT best practices, including:

- The need for a greater return on IT investments. As IT increases in complexity and operational value, its investments are being viewed along the lines of other business expenditures. Business owners and shareholders are now demanding that IT delivers measurable business value.
- The need for increased IT governance and control. Organizations face more and more regulatory requirements as the “cost of doing business.” Whether it’s Sarbanes-Oxley for public entities, HIPAA for health care related organizations, GLBA for financial services businesses, FDA for product and lot traceability issues, PCI and CISP for credit card processing, or other regulatory concerns, the need to meet regulatory compliance requirements is no longer just for “the big boys”. Most businesses today have some level of regulatory or compliance oversight that they are responsible for maintaining.
- The need to remain competitive with business peers. IT is a critical component of business operations. The organizations that “do IT better” than others inherently have a competitive advantage. Enabling business performance, as well as maintaining and securing information and minimizing business risks is as much a part of IT activities as fixing a broken printer. Falling behind in IT performance can directly impact business results.

IT best practices, standards and controls also help to prevent negative business impacts due to project failures, wasted investments, system crashes, security breaches and other IT related events.

Further, well disciplined IT organizations can also produce significant cost savings over their undisciplined counterparts. For example, according to Gartner, typically organizations can save 20% in terms of total cost of ownership ("TCO") for IT assets through server consolidation efforts³. This endeavor can also free up IT resources to work on new and more strategic projects and activities, rather than working on maintenance tasks. Many mid market businesses have large cost savings available to them if IT can "pick it heads up out of the weeds" and think rather than react.

Gartner further states that the implementation of IT operations process models, such as ITIL, can result in overall IT operating cost savings of 20 to 30 percent over three years⁴. This is due to the fact that organizations operating under a more mature, best practice model can often "do more with less" due to the consistency of processes within the organization. Unplanned events can be minimized, and IT resources can be reallocated to more strategic, potentially revenue enhancing activities.

Indeed, organizations that are made up of more flexible, strategically focused staff are more able to move talent around as needed to, for example, adopt new technologies. The more siloed IT organizations are inherently more costly to

run because skill gaps in these organizations must be made up by additional staff or contractors.

It is clear that well disciplined IT operations rely on operating frameworks to guide its processes, standards and controls. There are many flavors of IT operations and control frameworks, and two of the more "mainstream" models are CobiT and ITIL.

IT Service Management And Control Frameworks: A Primer

As previously discussed, GAAP, the principles governing accounting practices, have been used by businesses for more than 500 years. Compared to Accounting, the field of Information Technology is in its infancy, particularly from a standards and controls perspective. IT operations and controls frameworks have been established for less than 25 years, and have only become truly established in mainstream businesses in the last 5 or so years.

One major impetus for establishing and maintaining IT controls was the Sarbanes-Oxley Act of 2002. Sarbanes-Oxley ("SOX") was passed by Congress as a result of the financial difficulties endured by such companies as Enron, WorldCom and Adelphia. A key component of SOX was the requirement for an IT controls framework to manage IT operations as it interacted with the financial operations of a business. The merits of SOX can be debated, but for publicly traded companies, it cast light on an area that was largely ignored and misunderstood within the business. And for privately held companies, it raised a similar awareness of the impact of IT on financial performance.

CobiT

While a number of control frameworks existed, the Public Company Accounting Oversight Board (“PCBOA”), in conjunction with the Securities and Exchange Commission, established CobiT as the de facto standard for IT controls. Specifically, CobiT provides maturity models for control over IT processes. The framework provides a set of 34 high level control objectives, one for each defined IT process that are grouped into four domains: Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor. These groupings cover all the major activities performed by IT operations on a daily basis.

The CobiT model also provides an IT governance structure that links IT processes, resources and information to enterprise strategies and objectives. The governance framework provides management direction for getting the organization’s information and IT processes under control, monitored and measured against the organization’s objectives and performance benchmarks.

As opposed to CobiT, which is focused on the control and monitoring of IT activities, other frameworks, known as IT Service Management (“ITSM”) models, focus on the processes that manage the delivery of IT services to an organization.

ITIL

The most well known of these frameworks is ITIL (“Information Technology Infrastructure Library”). ITIL is a framework of “best practiced” based approaches to facilitate the delivery of IT services. ITIL outlines an

extensive set of management procedures that are designed to support organizations in achieving quality and value in IT operations.

Developed initially by the United Kingdom’s Central Computer and Telecommunications Agency in the 1980’s, ITIL has been revised and updated over the years. The latest ITIL version, Version 3, became available in 2007, and this has now become the standard for establishing IT operations processes and standards within an organization. Many organizations have adopted ITIL, although the mid market is certainly a “late arrival” to the IT standards bandwagon.

The core operational processes of ITIL include:

- Service Support
- Service Delivery

The processes of Service Support described in ITIL include:

- **Incident Management:** the process to restore normal service operation to the business as quickly as possible, and minimize the impact on business operations.
- **Problem Management:** the process to resolve the root cause of recurring incidents and minimize their impact to business operations, and prevent their recurrence.
- **Configuration Management:** the process to identify and track all individual components (Configuration Items, or CI’s) in the IT operating environment.

- **Change Management:** the process to control all changes to the IT operating environment, in order to minimize the impact of change related incidents on business operations.
- **Release Management:** the process to control the distribution of software and hardware across the IT operating environment, in order to control the distribution and installation of changes to the IT operating environment, and effectively communicate and manage expectations during this process.
- **Service Desk:** the single point of contact between users and IT Service Management to streamline communication and manage the life cycle of service requests.

The processes of Service Delivery described in ITIL include:

- **Capacity Management:** the process to align IT resources with business demands, and ensure cost effective provisioning of IT resources.
- **Availability Management:** the process to align IT service availability with business demands to ensure service availability at a justifiable cost to the business.
- **Financial Management for IT Services:** the process to provide cost-effective stewardship of the IT assets and resources, and to account for the spending on IT services and assets, in order to assist management decisions on IT investment.
- **Service Level Management:** the process to provide for the continual

identification, monitoring and review of IT service levels, as specified in Service Level Agreements (SLA's) to ensure that the agreed upon IT Services are delivered when, where and how they are supposed to be delivered.

- **IT Service Continuity Management:** the process to ensure the availability and rapid restoration of IT services in the event of a disaster.

This brief primer on CobiT and ITIL is not to "get technical" with the reader. Instead, it is designed to ensure that the reader understands the benefits of IT processes, standards and controls in the context of the well disciplined vs. the poorly disciplined IT organization.

IT Service Management And Control Frameworks In Undisciplined IT Operating Environments

In poorly disciplined IT organizations, most of these processes and controls are problems within the IT operating environment. Each represents issues that, if not well managed, can adversely affect a business. In the poorly disciplined IT environment:

- **Incident Management and the Service Desk** are often ad hoc processes, poorly documented and generally reactive in nature. Incidents can linger, causing longer business impact, and the less critical ones often "slip between the cracks". Unresolved issues, while not bringing down business operations, can impact business performance, and eventually, if remaining unresolved, result in increased performance degradation or even system outages.

- **Problem Management** is rarely performed, as this requires the recognition of recurring issues and the disciplined root cause analysis, rather than the constant re-application of “bandaids” to temporarily resolve these issues. More time is ultimately spent on resolving issues, and more significant problems can occur, as these recurring incidents are often symptoms of larger issues with the existing infrastructure.
- **Configuration, Change and Release Management** are also rarely followed. Infrastructure environments tend to be poorly documented, and changes take place without proper oversight, control and communication. The impact of this is felt in many ways, including difficulty upgrading and changing IT infrastructures, poor understanding of the alignment of technology components to business operations, and reactive, near-sighted support services.

Service Delivery processes are even more problematic. These processes, designed to help the business match IT resources to business requirements, and cost effectively acquire, implement and manage them, are generally reactive in poorly disciplined IT environments.

Undisciplined operations, by definition, involve little planning, and the planning that does occur is often done in silos. Service levels, when defined, are poorly monitored, and key IT performance metrics are either absent or unclear.

Without defined services levels, business executives often struggle to understand the impact of IT performance on the business, resulting in Infrastructure investments that are made with little regard for long term business strategy. When these investments are not viewed in the context of business value, they often result in smaller expenditures that ultimately do not meet the needs of the business. The business typically will not understand the reasons that greater investment levels are warranted, and suffer the consequences from poor performance, prolonged outages and wasted resources.

Culturally, poorly disciplined IT organizations also do not have the structure or direction to effectively adopt and enforce IT standards and controls. Although every IT organization strives for efficiency, effectiveness, and performance, operational discipline, and ongoing executive commitment, are required to achieve these objectives.

Any of us who have said “I will do better”, knows the pitfalls of proclamation without promise. The promise of change, without the commitment to change, is futile. And this applies to operational frameworks. There are many organizations that have invested significant dollars in adopting operating models such as ITIL or CobiT, expecting some “silver bullet” solution to their problems. But these frameworks can be so broad and encompassing, and without a standard prescription for implementation, that poorly planned implementations, combined with an uncommitted organization, can result in a huge waste of time and money, or worse, an organization that is more dysfunctional than when it started.

IT organizations that struggle operationally, cannot wave the “magic wand” of process improvement. Improvement comes from within and without. In the poorly disciplined IT organization, IT Standards and Control frameworks will largely be ineffective without a strong commitment throughout the organization, starting at the top. So, the culture must change along with the processes.

IT Service Management And Control Frameworks In Well Disciplined IT Operating Environments: Processes, Technology And People

Processes

In well disciplined IT organizations, ITIL based processes and controls are enablers within the IT operating environment.

By definition, well disciplined IT operations have the proper mind set and, well, “discipline”, to be successful implementers of frameworks like ITIL. All organizations have established processes, even if they are informal and undocumented. Well disciplined IT organizations may operate in an ad hoc manner, but they will be consistent in their application and diligent in their management. Implementing frameworks such as ITIL into these organizations will help them get to the next level: IT services that are clearly defined, measurable, well managed, understood by and effectively aligned with the needs of the business. They achieve the level of Business Effective Technology.

In a Business Effective Technology environment, IT services and service level requirements are documented in a Service Catalog that defines the services to be provided to the business, and metrics to measure their effectiveness. Service level agreements (SLA’s) are established between IT and the business, and clear accountability is determined. Lines of communication are built that facilitate, not just incident resolution, but more importantly, the ability of the business to engage IT in strategy discussions to support the goals, objectives and vision of the business. IT becomes a true business partner, and in today’s technology consuming world, the business cannot be effective without this partnership. That is the true definition of Business Effective Technology.

Technology

Beyond services, well disciplined IT organizations have the tools to support its objectives. “Tools”, in this definition, are categorized in two ways:

- Service Management Enabling Software (“Technology”)
- Highly Qualified and Experienced Resources (“People”)

Two types of tools are essential for Business Effective Technology. They include:

- Service Management Software
- Network Monitoring Software

Service Management Software facilitates the ability of the organization to record, track, resolve, and communicate on issues that arise.

Service Management Software is a major component of the Service Desk, helping it to manage incidents and problems, record and document the infrastructure environment, and oversee change within it. But Service Management software is more than a Help Desk System. A key element of Service Management Software is the Configuration Management Database ("CMDB").

The CMDB defines the different "pieces" that reside within the IT infrastructure. Known as a Configuration Item ("CI"), a CI is any component that is a part of the IT environment that has configurable attributes. The main purpose is to identify these components and their relationship to the other items in the environment. Examples of CI's include servers and software; even the people that use these components are considered "CI's".

The value of the CMDB is that it not only identifies the CI's in the environment, but the inter-relationships of all of these elements. Software is installed on computing devices that are used by people, supporting specific business services, residing in specific locations. All of these elements depend on each other to work effectively. If one "link in the chain" is weakened, it can break apart the whole chain.

Computing and systems are so reliant on the various components that comprise it, and information on these components is critical to quickly resolving a support event. Like the old poem,

- For want of a nail the shoe was lost.
- For want of a shoe the horse was lost.

- For want of a horse the rider was lost.
- For want of a rider the battle was lost.
- For want of a battle the kingdom was lost.

Computer systems are much the same way: For want of a \$100 network switch, connectivity was lost, creating a system outage that resulted in millions of dollars in lost revenue. Extreme? Perhaps, but it has happened. Will it happen to you? Has it?

The CMDB provides accurate information on and documents all of the IT assets and configurations within the organization and its services. This information enables the Incident, Problem, Change and Release Management processes, thus facilitating the root cause analysis and issue resolution process. Incidents, events, and problems can be resolved more quickly, before business impact is significant. Business Effective Technology relies on it.

In addition to Service Management software, Network Monitoring software helps IT more effectively respond to issues that impact the business. Effective network monitoring is more than "up/down", identifying when something in the IT infrastructure is "broken". It establishes and measures performance thresholds for devices in the infrastructure to proactively notify IT of changes in the environment that may impact performance or availability before an outage takes place. This changes the IT support paradigm from "reactive fire fighting" to proactive performance and analysis, and increases IT's visibility over its "terrain".

Combined with Service Management software and the CMDB, the IT organization has a better understanding of the entire infrastructure and its relationship to business services, down to an individual user level. In a Business Effective Technology environment, these tools are fully integrated, allowing IT to better understand the issues that are occurring in the infrastructure, and how they affect business services. It can more quickly assess these issues to resolve them before the business is affected.

Mid market IT Departments are certainly aware of the technologies that exist to support Business Effective Technology. However, the investments that are made are usually at the lower end of the solution scale, and often are siloed, providing isolated snapshots of the technology. We have seen companies that have invested in more than 30 different monitoring tools, each looking at different components of the IT architecture. This can result in "information overload", with IT unable to "see the business forest for the technology trees." Like those 3-D paintings, with technology you often need to "step back" to truly see the whole picture.

Many mid market businesses struggle with establishing and implementing effective processes to manage IT services and delivery. This issue is compounded by the lack of robust tools to support these processes. In the well disciplined IT operation, strong, managed processes are combined with the right technologies to give IT the needed window into the business and its related technology to effectively support business services.

People

The third "piece of the puzzle" to Business Effective Technology is the People. In well disciplined IT organizations, the right people, with the right experience, are available for the right roles.

Too often, mid market companies struggle to hire and retain the IT industry's "best and brightest". To be blunt, the technology environments are often not "hot" enough to attract the talent needed to support it. And the level of demand for this talent pushes the compensation levels in the industry to ranges that make it difficult for mid market companies to support.

This often results in high turnover in the IT organization, as high performing resources move on to "greener pastures", and underperforming resources are forced out. High turnover creates disruption in the IT organization, as often the business' technology knowledge goes with it. When the environment is poorly documented and siloed, employee turnover can magnify the support and change issues that already exist.

In addition, "reactive" IT environments are typically more stressful than well managed, proactive ones. The increased stress and pressure in the environment can cause employee dissatisfaction and performance issues, further increasing turnover rates and reducing service level effectiveness.

Many mid market companies also can experience the other end of the spectrum: IT staff that never leaves. While employee stability sounds like a good thing, in IT, bringing in "fresh blood" helps a business

stay current with technology changes. And too often, long-standing IT employees become the “guardians of information” rather than its disseminators.

We have all seen the situation where a long time IT employee, in a poorly documented environment, controls information and systems, and doles it out according to his or her own agenda. Like the “troll under the bridge”, these IT resources will not provide the answers the business needs, unless the business has the appropriate “password”. Give the wrong answer and you can end up as “lunch”. No business should be held hostage by any employee, but for some reason, it is sometimes tolerated within IT. It shouldn't be.

In the well disciplined IT environment, people operate in well defined roles that fit the needs of the technology that best supports the business. These individuals have the right experience, credentials and attitude. They also have the appropriate performance measures and incentives that are aligned with the overall objectives of the business. They are measured and managed accordingly, and are held to a standard of performance.

In the well disciplined IT operation, the company's IT staff is given an environment that enables its success, with the appropriate processes and tools in place to sustain it. They are empowered to do their jobs, and have the versatility needed to support a broader range of business and technology services. The silos come crashing down, as all functions are effectively managed, with the technology and business inter-relationships defined and integrated.

And this goes beyond the IT organization. The well disciplined IT organization needs the support, the attention, the active involvement of the company's leading business executives. The cultural barriers and poor communication that often isolate IT from the rest of the business must be removed. To paraphrase former President Ronald Reagan, “Mr. CEO, tear down that Business/IT wall!”

According to the MIT Sloan Management Review, key executives must ask some of these key questions⁶

The CEO

- How important is IT to the business operations and to the business strategy?
- How knowledgeable is the business about IT?
- How knowledgeable is IT about the business?
- Who is responsible for making key IT decisions, and how can they be made accountable?
- What are the key metrics that will help define how to get the most value from IT?

The CFO

- What are the key IT assets within the business?
- How are these key IT assets tracked, managed and maintained?
- How can the business make better IT investments?
- What level of investment does IT really require to support the business operations?

- What level of future investment does IT require to support the business strategy?

The Business Unit Leader

- How much do the business processes rely on IT services?
- How effective is the partnership between the business unit and IT?
- How knowledgeable is the business unit about IT?
- How knowledgeable is IT about the needs of the business unit?
- How are key IT decisions made in the business unit?

The HR Director

- How effective is the business at attracting and retaining IT talent?
- What are the key values, credentials and experience required for IT success in the business?
- How is the performance of IT resources measured?
- What incentives exist within the business to ensure an open business/IT culture?
- How effective is the business' professional development for IT resources?

The CIO

- What are the key IT assets within the business?
- How are these IT assets allocated across the business?
- Are these assets properly aligned with business performance?

- How dependent are business processes on IT services, systems and performance?

- How well does IT prepare for and mitigate business risks that are dependent upon technology?

When all of the primary elements of Business Effective Technology are in place, with the proper processes and a service management focus, the appropriate tools integrated to these processes, the right people with the right attitude, and an enabling, open culture, a well disciplined IT organization will be established. And the business will benefit.

Making It Work™: The Path To A Well Disciplined It Operation

Effective IT processes support communication, issue resolution, technology change and business/IT alignment. This is not to imply that implementing a framework like ITIL is like talking a walk down "Main Street, USA". It is not a simple, idyllic, well manicured solution. Not without, work and commitment.

A framework such as ITIL is not "one size fits all". It needs to be tailored to the individual requirements of the business. Adoption of IT Standards and Controls need to be consistent with business objectives and needs. To avoid costly and unfocused implementations, and to ensure that the processes are effective for the needs of the business, several steps must first be taken.

- Align IT operations with business goals and strategies.
- Analyze current IT capabilities and identify operational gaps.

- Determine which processes are most important and effective for the business, and prioritize their adoption.
- Ensure that these processes are well understood by the organization in advance of their adoption.
- Establish a strong business sponsor who will take responsibility for communicating, mediating and enforcing established IT Standards and Controls.
- Understand and define the risks, and determine mitigation strategies.
- Define expected outcomes and establish methods to monitor and measure results.
- Continuously assess performance against expectations and remediate any deficiencies.

Many mid market business executives, used to operating in a wide open, ad hoc IT environment, often make the argument that strong IT controls and processes will make it more difficult on them. They are afraid of limiting their ability to do their jobs, and creating an unwieldy bureaucracy to govern IT needs. If an IT service management framework is adopted, without understanding its role within the business; if it is not adapted to the demands and daily operations of the business, then this situation can occur.

But is it “bureaucracy” to demand that change be planned and managed, and risks controlled? Is it “bureaucracy” to require that IT investments be made with proper evaluation and oversight? Is it “bureaucracy” to insist that the business reliance on IT be understood, assessed and

properly allocated? Is it “bureaucracy” to establish an open, unencumbered and meaningful dialog between the business and IT?

It is difficult to understand how establishing appropriate performance expectations and operational discipline, increasing visibility over performance, improving communication and measuring results can have a negative impact on a business. Other departments within the business have these standards and measures in place. There is no reason for IT to operate without them, as well.

Conclusion

Making IT Work involves effective communication, performance, discipline, management and capability. As technology evolves and becomes more integral to successfully competing in today's business world, poor IT performance can be devastating to a business. A key question to business executives today is not, “Can you afford to invest in improving your IT performance?” but instead is “Can you afford to not invest in IT improving IT performance?”

Just understanding the impact of poor IT performance is a great first step. But understanding the importance of a well disciplined IT operation in improving business performance is a better step.

When evaluating the state of your IT organization, keep in mind that you cannot transform your organization alone. IT Managed Services is a valuable mechanism for achieving business transformation,

enhancing business agility and managing IT operational costs.

The definition of "IT Managed Services" is a critical part of the equation. If IT needs to be more than "putting out fires", then IT Managed Services needs to be more than "break and fix". It should include the following key elements:

- Defining appropriate IT performance expectations and service levels
- Implementing effective IT standards, processes and systems to monitor operations and performance
- Understanding the impact of IT failures and mitigating the risks
- Establishing realistic and flexible IT cost, investment and business alignment strategies
- Leveraging key technical and operational expertise when you need it

IT needs to be understood and managed just like any other part of your business. If you believe that preventing "fires" is a much more effective business approach than "putting them out", then you must understand how IT fits into your business plans.

Based on this plan, develop appropriate funding, establish structured and disciplined IT operations, define specific performance objectives that are measurable, and understand and plan for the impact to the business from IT outages. The results will be improved productivity, satisfied business users and customers, effective IT cost

management, and an IT operation that is focused on the needs of the business, today and in the future.

Notes:

See, "A Checklist for Process Improvement: Metrics that Matter" by Gene Kim, Enterprise Systems, March 27, 2007

2 See, "IT Managers Feel the Firefighting Heat?" IT News, June 27, 2007

3 See, "Frequently Asked Questions About Techniques for Reducing IT Costs" by Barbara Gomolski, Gartner, September 18, 2006

4 Ibid

5 See, "IT Refresh Statement" (<http://www.ogc.gov.uk/refresh.htm>), Office of Government Commerce, May, 2005

6 See, "Generating Premium Returns on Your IT Investments" by Peter Weill and Sinan Aral, MIT Sloan Management Review, Winter 2006, Volume 47, No. 2



About Auxis:

Headquartered in Coral Gables, FL with offices in Plantation, FL, Atlanta, GA and Washington, D.C., Auxis is a management and technology consulting firm that creates value by enabling growth for its customers. We offer a multi-disciplined approach to develop and implement practical, robust and scalable solutions that generate superior business performance, providing significant competitive advantages to our clients. Our core belief is that our success should be measured by tangible and sustainable financial results. Simply put, Auxis helps clients prosper.

Auxis understands that today's technology is increasingly difficult to manage and support for most businesses. For Auxis, IT is our vision, our mission, and our passion. We make IT Work. To learn more about how Auxis Managed Services can help you Make IT Work, visit us at <http://www.auxis.com>.

Headquarters

55 Miracle Mile, Suite 300
Miami, Florida 33134
(305) 442-0060

www.auxis.com

Ft. Lauderdale

7901 SW 6th Court, Suite 130
Ft. Lauderdale, Florida 33324
(954) 236-6682

Atlanta

3500 Lenox Road, Suite 300
Atlanta, GA 30326
(404) 419-2215

Washington, D.C.

1701 Pennsylvania Ave, Suite 300
Washington, D.C. 20006
(202) 390-8606