



# Process Matters: Don't Abandon Your Critical Infrastructure!

By Kevin Behr

---

## Executive Summary

Is your team finding it hard to balance an ever increasing workload of projects along with demand oriented daily operations? Are you considering managed services to offload the mundane aspects that are bogging your team down? Do you have that foreboding sensation in your stomach? Are you worrying about what details may be missing from all the proposals you have requested? Why does it seem like many of the managed providers you have spoken with are merely coin-operated real estate agents? How come "I am sure we have dealt with that before" is not an acceptable answer when your team asks about operational specifics? You know the clock is ticking and you can't put off action any longer. What do you need to know to make sure your decision is correct? How can you avoid a costly and embarrassing situation that you may have to live with for years? In this paper we reveal the absolute **must have** elements of a complete managed services program. We calm your fear with knowledge by giving you the inside look at a thriving operations program. Step by step we outline the critical processes and controls your provider must demonstrate mastery over in order for you to be successful. You can then ask relevant questions of any service provider and get the answers you need to make the best decision period.

## How Can We Get Back On The Right Track?

In the realm of Information Technology, work falls in to one of two categories. The first category is operations, which is responsible for running the IT systems already in place. We are all well familiar with it as it takes up most of our time - in many cases up to seventy percent of an IT budget. Every new IT system includes a lasting commitment to ongoing maintenance and support. This ongoing effort generates countless hours of unplanned work. The ongoing response to unforeseen situations that demand a response makes it extremely hard to find time to get to the second category, projects, often referred to by beleaguered IT pros as "the work we meant to do". This is the work that supports the changing needs of the business. And in a dynamic and growing business, the ongoing stream of project demands should be a top priority for IT.

Many organizations have already engaged in the search for a service provider to offload the operations of their critical systems, freeing up more internal resources to focus on strategic new projects that support the changing needs of the business. Not all service providers are created equal. And for a hard charging IT organization that may be considering the services of a 3<sup>rd</sup> party to help manage critical business systems, the choices can be daunting.

What do you need to know in order to choose a service provider that actually delivers and doesn't cause more headaches than maintaining the infrastructure yourself?

## Consider the Conflicting Demands of the Typical IT Shop

We have all been there. It's four-thirty in the afternoon, where did the day go? Instead of having time to work on the most urgent project, you find yourself buried in mundane operational quagmires. Every day starts to feel the same. Why aren't the must-do projects getting done? If only it was a single reason. Viruses, spy-ware, server crashes, flaky new applications and all of those machines that need patching. Even if you could afford to hire more network engineers and really smart people, the backlog would certainly continue to increase. Never mind the fact that you are probably getting heat for the amount of IT staff you already have. Why does it feel like



you could throw a huge team at the ever changing needs of the company, and you would still not meet them all?

Why is it that day after day your brilliant team spends close to eighty percent of its time fighting fires? Why does it take your most seasoned network guru to fix a measly broken printer? Maybe because everyone else is up to their eyeballs in tickets and the printer is connected to the network. It could also be that the printer belongs to a VP of Marketing and his assistant just ordered you to send your best person to fix it right away.

Does any of this sound at all familiar? Balancing projects and operations can feel like walking a high wire even on a good day. Especially when there is a substantial disconnect between the demands of the operating environment and the level of process a growing company's culture will tolerate.

Never mind that you don't have the time to really get to the bottom of system issues; your team is often forced to reboot servers just to make the symptoms disappear. The inability to ferret out true root cause in many outage scenarios is often compounded by the lack of a duplicate test environment. This leads to experimentation with production infrastructure during an outage in a desperate attempt to reverse the outage. This theory testing often creates new issues worse than the original outage. These are tough concepts for many business executives to grasp during budgeting when test systems are often requested. In many situations these are the first initiatives to be sacrificed in order to get to a more acceptable budget number.

## **Betting on a Proven Approach**

Volumes have been written by analysts and IT researchers about the causal factors of IT outages and downtime. It should come as no surprise that people and process issues are the number one factor in outages and downtime. In other words, who changed something?

What kind of environment is needed to reduce the constant demand of operations on your IT team? The key words are operational maturity. Whether you consult the latest benchmark research from the IT Process Institute, Inc. [www.itpi.org](http://www.itpi.org) read work The Uptime Institute <LINK> has done, or check out the scores of reports from leading industry analysts, you will find a similar theme. High performing IT operations teams possess a well-defined set of processes and controls that are enforced with rigid resolve on a daily basis. For example, Microsoft found that its high performing customers rebooted their servers a fraction of the time of the average IT organization. Why? Because their defined processes and controls allowed them to isolate the true root cause of failure and use this knowledge to avoid encountering the same issue repeatedly. These advanced processes and controls zero in on prevention of outages in the order of their causal likelihood. High performers know most outages are not caused by power or hardware failure. So while physical infrastructure redundancy and good architecture are necessary, they are far from sufficient when it comes to protecting your executives from critical application outages.

Hallmarks of such structured organizations include practices such as end-of-shift audits. These audits require that the leaving shift hand the datacenter over to the arriving shift in the exact same condition it was left in. That means that any changes to anything must be approved, documented, and presented to the arriving shift manager before the ending shift can go home! Such practices may seem draconian, but these carefully evolved systems enable continuous operation at efficiency and effectiveness levels that most IT shops can only dream of.

The bottom line is that to maintain your mission critical applications and enabling infrastructure, you need to build a stable and repeatable operations environment like the high performers use. By environment, we are not talking about building a datacenter or buying HVAC to cool it. (Although in many cases, you can justify working with a managed hosting provider on the cost savings associated with not having to build out the physical environment alone.) The real payoff is



in the continuity of uptime, which translates directly into a major reduction in distractions for your IT team!

But many IT professionals know that re-engineering a company's IT operation is both expensive and time consuming. Many companies will require outside expertise, and since IT touches every facet of your company, so will the changes you need to make. Processes at the core of high performance - such as Change Management - will have a ripple effect, touching many stakeholders well outside of IT. You will need business buy-in on these improvements from key executives throughout your entire company.

Furthermore, there is often a cultural disconnect between stable operating environment needed to optimize system performance and the dynamic environment found in the typical growing business. In dynamic organizations it can be very difficult to implement new process and controls around the production environment. Process improvement itself becomes another project competing for the same resources as daily operations. In addition, the highly skilled IT generalists who have responsibility for multiple areas within your IT shop are not naturally a good fit for a rigorous process and procedure focused environment that is proven to optimize system performance.

As if the requirements of your company aren't enough, if you are in an industry or sector that is regulated by any authority, you will need to make sure you factor meeting additional external requirements and generating acceptable proof of this compliance. This can be a daunting task when your organization is growing and dynamic. Formal processes are a rarity, and documentation of existing ad-hoc processes may be scarce.

## Pick a Solution That Matches the Problem

Part of the struggle lies in the oppositional nature of projects and operations. A successful project team is able to make many changes. A successful operations team is trained to resist changes as they are the source of most outages. If you find your IT organization in the middle trying to implement new projects but also trying to protect the existing production environment, you are acutely aware of this dilemma. Projects and operations have competing values at their very core.



High performing IT operations teams such as the award winning team at IP Services have built a highly effective and efficient set of IT Operations processes, instrumented with carefully chosen controls that reflect the true risks of the environment. These processes are outlined in the ITPI's best selling book, *The Visible Ops Handbook*. IP Services has lead managed hosting providers by adopting and integrating industry best practices as outlined by the IT Infrastructure Library (ITIL) and the comprehensive control framework of Control Objectives for IT (COBIT), created and published by the Information Systems Audit and Control Association (ISACA). In short, we have chosen to optimize our organization for IT operations period.

This approach represents a radical departure from the normal hosting data center environment. Most hosting centers simply provide real-estate for your infrastructure and remote bodies to perform simple tasks at your direction. This is a far cry from settling your infrastructure into an effective process and control operations plan. The typical hosting provider environment still requires your organization to do all of the actual work and direct the remote technical resource to



do it on the other end of the phone. In essence, remote hands services, devoid of a comprehensive operations plan, create more work than they can ever accomplish alone.

While many organizations are lured into hosting because of the purported cost savings, the actual results can be underwhelming. Hosting and outsourcing industry insider phrases such as “Your Mess for Less” tell the real story. Without the appropriate preventive, detective and corrective controls to gauge the effectiveness of the provider’s operational processes, it is very difficult to measure the hosting providers’ performance. If you ever wondered why the uptime and Service Level Agreement sections of their proposals seem more like actuarial calculations than business metrics, now you know. They probably lack a controlled and successfully instrumented operational environment. Furthermore, when the provider gives you “uptime” statistics, be very wary. Are the statistics based on actual holistic operational and application performance, or simply network device availability based on ping data?

Succinctly said, mission critical applications are most effectively managed by IT organizations that have made serious investments in process, automated workflow, a system of relevant controls, and automated instrumentation of those critical controls. When choosing your managed hosting partner, make sure that they can demonstrate such a system to you! If they can’t, or tell you that they are sure they have this because they support huge clientele, don’t be fooled. The proof is the system. They either have it or they don’t. Many providers don’t.

## **A Word About Infrastructure**

While people and process issues embody nearly eighty-percent of the causal factors for IT outages, hardware and environmental issues represent fifteen to twenty percent of the total. This qualifies environmental issues as the second leading cause of outages overall. Physical redundancy is the most visible form of hardening and is really where most hosting providers focus their sales and marketing efforts. Most providers love to wow IT executives with tours of their massively redundant facilities. When have you ever been offered a tour of the provider’s operations process and control environment? It seems crazy not to address how your team will prevent nearly eighty percent of outages. It seems even crazier to select a service provider that is focused on creating a physical environment that addresses the causes of only fifteen percent of outages. Process and control flow should dictate how the physical environment is built. After all, the physical environment must be maintained proactively to be reliable.

The massive expense associated with the design and build-out of a data center is what starts many IT teams searching for a hosting provider when their organization is growing. Many company’s cramped data centers are almost out of space by the time the data center is completed so scalability concerns enter in to the picture. Scalability is by far the most costly hidden feature of a data center. Scalable power, cooling, and bandwidth all add up because closed-end solutions can not be used. Everything must have an upgrade path. Throw in the multiplier for redundancy at all of these critical points and the price tag becomes unrealistic for the average growing company.

To really reduce the risk of environmental and hardware issues you will want to ask your managed hosting provider if they can help engineer the hardware and environmental aspects of your hosting solution based on their experience. This should include specific recommendations based on your company’s unique needs and applications. Your service provider should also be able to give you straight advice about which brands and models of infrastructure work best. Remember, they should have extensive records of failures and outages in their various support tools to back this up.

From an initial cash outlay standpoint, it certainly makes sense to locate your critical infrastructure in a hardened data center. Many growing companies would never be able to justify the elaborate and expensive environmental redundancy on their own. But choosing a data center



devoid of a comprehensive operations plan will result in disaster or in the best case, the same issues you have now, except the infrastructure will be much farther away.

### What Processes and Controls Should I Look For?

High Performing IT organizations demonstrate mastery over all three categories of controls. The control categories are Preventive, Detective and Corrective. In these organizations, the goal of IT operations is to do everything reasonably possible to prevent outages, to monitor key indicators of issues that may lead to outages, and in the event of an outage, to restore service as quickly as possible, taking appropriate proactive learning steps to ensure the outage never reoccurs.

Control Type	What it does	Example
Preventive	Stop undesired outcome from occurring.	Changing oil in a car avoids unnecessary wear and tear on the engine.
Detective	Alerts when a set of predetermined conditions are met	A fire alarm detects high temperatures and smoke then emits a loud noise to alert of potential danger.
Corrective	Reverses an undesirable outcome	A mechanic fixes a leaky radiator in a car by installing a new one.

### Preventive Control

In order to prevent outages, your service provider must demonstrate an effective plan that outlines a preventive maintenance process complete with controls to measure its success. This program must represent regularly scheduled activities that are broken down into batches of compatible activities. At IP Services we call these groups of preventive activities work packages. The work package process is integrated into our own best practices inspired workflow system called Interchange. By using a single system to schedule the execution of work packages, Change Management, Incidents and Problem management our operations team has complete visibility into activities that affect your infrastructure all in one location. Interchange can even be configured to allow your IT team to participate in these processes and leverage them in your own operation virtually anywhere in the world! Our internal controls system monitors the work package process for effective compliance. We measure the ability of every engineer to complete all assigned work packages in the time allotted. This provides you with a high level of assurance that the preventive work is getting done consistently.

Change Management is another preventive control that must be addressed by your provider. If your service provider does not include your staff in Change Management meetings and or decisions then run do not walk away! Change Management is not just a process but rather is a culture taken very seriously by high-performers. Since change and risk are often synonymous the ability to effectively manage change together is crucial to your company's ability to achieve any kind of gain from managed hosting. In order to demonstrate true compliance and guard against unauthorized change your provider must integrate the preventive control of change management with a detective control that continuously monitors the configurations of all key infrastructures for change.



## **Detective Control**

If nearly eighty percent of IT outages are caused by humans, then a system of controls around human interaction with IT infrastructure is critical to reducing the rate of occurrence and length of IT outages. Not only do statistics show us the cause of outages, but studies also show that eighty percent of the time it takes to repair an outage is spent determining what changed to cause the outage. Developing a baseline of key configurations of your infrastructure and monitoring them continuously for any change is an effective detective control. In an outage situation we can quickly determine whether the service interruption is the result of an activity related to change, or if it represents a hardware or software failure. We can do this in minutes, not hours. This gives us the ability to reduce the Mean-Time-To-Repair (MTTR) and also aids in the forensic style activities associated with determining root cause. At IP Services, we have the ability to reconcile every detected change against a list of approved changes. This determines whether or not the change represents authorized activity. If the change is found to be unauthorized, we can then roll it back and investigate the source of the change.

## **Corrective Control**

In the case of a service interruption, you will need to depend on the corrective controls of your service providers. Make sure that your providers' corrective controls are based on best practices such as those outlined in Visible Ops and the IT Infrastructure Library. Ask for a process flow description, and make sure to break it down into pieces you can understand. You should be able to discern the critical restorative processes. At IP Services, we have adopted Visible Ops and ITIL as part of our best practice framework. The ITIL calls these two processes Incident and Problem Management. The difference between an incident and a problem? An incident represents an issue where the solution is known and can be implemented from a run-book or an existing body of knowledge such as a knowledge database. A problem is defined as a service impacting situation where the cause is unknown and must be determined in order to restore service. The ongoing goal is to turn problems into incidents by getting to the root cause of the issue and documenting the solution. Then proactively, projects to correct the issue on other relevant infrastructure can be planned and scheduled to prevent the issue from occurring anywhere else. Also if the problem does occur again, the outage time is reduced by the ability to play back the solution from the knowledge base rather than troubleshooting the issue all over again.

Additional gains are made by integrating the Change Management, Change Detection, Incident and Problem Management processes together. Since change is a large causal factor in outages, there is much to be gained by ruling it out early in the stage of an incident or problem. It can shave hours and sometimes days of wasted efforts off of the Mean Time To Repair. Make sure your provider has an integrated process suite based on industry best practices defined by ITIL and Visible Ops!

## **So What About Security?**

Most security experts agree that true security hinges on effective configuration management. Configuration Management is the stuff that gets the high performers excited. If you don't know what you have and how it is configured, then how can you defend it? Be very wary of so called managed security providers that have no operational component to integrate with the change management processes used to protect your infrastructure.

You will also want to be sure that while a security advisor should direct the work being done, an operations team should do the actual work. Separate teams performing work on your IT infrastructure is a recipe for outages followed by finger pointing. Look for an integrated approach to security. All security work should be subject to Change Management approval. Watch out for



security patches and make sure they are tested before they are rolled out on to your infrastructure! Be careful to understand how the provider plans to keep abreast of security patches, issues and the unique requirements of your environment based on its applications. If there is little or no integration of security into the operations regimen, how will you know that security work is included in regularly scheduled work packages? How will you understand the vulnerability management regimen? How will you get to say yes or no to proposed patches? These are all critical questions and the answers should be found in the operational system of controls.

## **Summary**

Partnering with IP Services, a high-performing managed service provider, represents the most direct path to move your critical applications into a tightly controlled and predictable environment. By choosing this path, you can enjoy the benefits of our continuous process improvement without the expensive, lengthy, and disruptive projects which are frequently associated with their implementation. Now you can enjoy the reward of increased availability, predictability and scalability by leveraging our effective process and control infrastructure.

From the perspective of a growing company, freeing up valuable operations bound IT resources to deliver on high-value projects is job one. It makes sense to trust the care of your mission-critical applications and their enabling infrastructure to a managed service provider such as IP Services.

At IP Services we are a benchmarked, continuously-audited, high-performing IT operations team. Let us help you meet your goals by operating your mission critical applications in our tightly controlled environment. Instead of building an expensive datacenter, move your infrastructure to ours! Free your team from mundane operations tasks and leave the boring repetition and day-to-day work to us. Remember the clock is ticking on those projects, visit [www.ipservices.com](http://www.ipservices.com) to contact an IP Services Sales Engineer and schedule an assessment of your needs today!