



2896 Crescent Avenue
Eugene, OR 97408
Toll Free- 866.226.5974
Phone- 541.353.5974
info@ipservices.com

The Mighty Fortress has an Achilles Heel

It takes more than a building.



The Mighty Fortress has an Achilles Heel

It takes more than a building.



If you are looking for a service provider to help your IT organization focus on more strategic activities by managing your mission critical applications and infrastructure, you need this information!

Many service providers believe that the best way to achieve high availability is to pack up your infrastructure and move it to their physically hardened and highly redundant data centers. Meanwhile the most likely risk to your success, specifically availability, is ignored and not discussed.

What if the millions upon millions of dollars many service providers spend on infrastructure...and even their service offering themselves...fail to address the root cause of nearly eighty percent of all infrastructure and application outages?

If you have ever visited a commercial data center you are sure to have been impressed with the sheer scale and massive money-is-no-object redundancy built in to most every facet of its physical infrastructure. From the moment you enter the facility and are photo-identified, patted down, stamped, badged, retina- and palm-scanned, the show is on.

Hosting vendors often love to give elaborate tours, explaining the incredible measures taken by the facility designers to ensure that the data center could sustain a near-direct nuclear detonation unscathed.

As you walk by a particularly large cage shrouded with black stealth-like racks full of sinister looking servers, the tour guide points at it and says "Here is where a major search engine company is based, of course we can't say who" and smiles. The tour guide will gladly stop to point out that the hosting company has invested more in their cable plant than your company earns in a year.

The combination of the fortress sensation and scale on steroids lures many IT executives into a false sense of security with regards to reliability. The majority leave the tour overtly impressed. Later, when it comes down to what services the provider can actually perform for their servers and other infrastructure, many IT staffers can't answer in specifics. If they can answer your questions, it's usually to tell you that the provider can patch your servers and help configure your firewall. The tour just felt, well, massive and powerful, and everyone wants to be big and powerful, right? Power means security, and that all translates into reliability somehow?

In fact many IT executives have a eureka moment when they find out that the likely cause for nearly eighty percent of IT outages has nothing to do with jet powered generators, tons of redundant HVAC, N plus one network failover, multi-homed connectivity or laser-powered wire-speed firewalls. The moment then turns to terror when they realize that what they have been sold has very little to do with what it is that they desperately need. Reliability.

The key to reliability is understanding failure and, more importantly, why it occurs. Studies published by many IT analyst groups, think tanks, and cutting-edge research firms provide clues to what causes IT outages.

IT outages are most often the undesired effect of work that IT staffers meant to do. Yes, it is true that all of the differing studies agree that nearly eighty-percent of all IT outages are caused by people and process issues.

More importantly, advanced research performed by the IT Process Institute reveals just what high performing IT organizations do differently than the rest to gain the reliability edge.

If IT outages are the unintended consequences of well-meaning IT organizations making changes to infrastructure, what are you to do? The answer is not to stop making changes! If all changes were halted, projects could not be implemented, no problem fixes would take place, in short nothing would get done. Conversely the organization where business as usual actions result in outages and fire-fighting the Ben Franklin adage applies “The faster I work the behinder I get.”

Who would have thought changes made to IT infrastructure could slay a Pratt and Whitney jet-powered generator with a guaranteed fuel delivery contract? It begs a powerful question. Does your provider understand this, and if so, how can they help you to address these risks?

For a minute let's go revisit the datacenter tour. Remember all of the impressive physical and network infrastructure you were shown? How much outage risk does it really remove? Given the focus shown by most hosting providers on physical infrastructure it becomes obvious that many simply don't get it when it comes to reliability. Environmental issues such as power, hardware and cooling are only responsible for around fifteen percent of outages, with security bringing up the rear at nearly three percent.

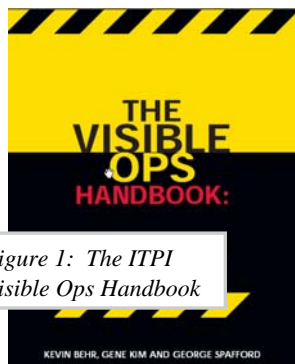


Figure 1: The ITPI Visible Ops Handbook

Clearly reliability and long term success of IT services hinge on the ability to operate infrastructure in a tight system of process and controls that begin by adequately addressing people-, process- and change-related risks.

The IT Process Institute recently completed a landmark research project entitled the IT Controls Benchmark. IT organizations of all sizes, scopes and across many industry sectors were benchmarked in several categories of processes and controls. The researchers were looking to correlate a distinct set of controls and processes with high performance. In the research, several high performers were identified and close attention was paid to what made them

different than the rest. Previously the ITPI had also published the Visible Ops Handbook that describes how to bootstrap several key processes and controls necessary to start down the



road of high performance. In the handbook it is clear that high performers not only walk their talk they actually talk differently than the rest. Because high performers understand where risk really comes from, they design effective process and control architectures. It is a case of function following form and it pays off in reliability. These organizations are virtually non-stop when it comes to uptime.

High-performers also have obtained a larger span of control. They are able to control the same infrastructure as others but with one-fourth of the staff. Did I mention they have much happier customers?

What's good for the goose...

So if most providers sell massive infrastructure as the cure for reliability issues, how do you get what you really need? How do you find a provider that focuses on risks to reliability based on their likelihood of actual occurrence? Who uses science to achieve the best overall approach?

It's one thing for the provider to understand risk and manage their own infrastructure correctly, but even if they do apply it internally, can they extend their world-class processes to your infrastructure?

It seems pointless to build a world class set of processes, controls and highly redundant infrastructure only to let your clients wither on the vine. Sound crazy? You would be surprised to see that this is the case in many commercial datacenters around the world. Yes, they can show you that THEY are never down but how about your infrastructure? Can your provider promise the same uptime guarantee with your infrastructure?

At IP Services we continually lead the industry with the creation and early-adoption of many best practices. These best practices have been adopted to reduce the risk of outages and failures in our IT service offerings. In fact, our radically different approaches to IT operations management led to the development of Visible Ops. We, along with Tripwire, the co-developer of the Visible Ops methodology, donated the entire methodology to the IT Process Institute. The IT Process Institute¹ is a think-tank dedicated to advancing the science of IT Management. They pursue these goals through rigorous research, benchmarking, and then developing prescriptive guidance. The IT Process Institute has since conducted extensive research into the methodology and published the Visible Ops handbook.

The handbook outlines a small subset of controls and processes that, when linked together, form the core of IT service integrity. This core is comprised of scientifically selected Preventive, Detective and Corrective controls to surround your infrastructure with protective layers of continual operation assurance. Visible Ops was carefully derived from the playbooks of high-performing IT organizations and codified in the Visible Ops guide published at the IT Process Institute. Gene Kim (CTO of Tripwire) and Kevin Behr (former CTO of IP Services) spent several years extensively studying high-performing IT operations teams to find out what separated them from the rest.

¹ The IT Process Institute's web site can be found here: <http://www.itpi.org>

What are controls and why do I need them?

There are three principle categories of controls we use at IP Services to provide you with highly reliable IT services.

Preventive controls are used to stop undesirable events such as outages from occurring before the fact. These events could be brought about by human causes or environmental causes, such as changing the filters on the datacenter HVAC unit and preventing a loss of cooling. Change Management is considered a preventive control as the judicious review, approval and scheduling of change activity is designed to prevent outages and interruptions to IT services.

Detective controls provide an alert that a desirable condition or state has changed. The detected change could be acceptable such as an approved infrastructure change that results in a new device configuration. The alert could also be due to unauthorized activity or a dangerously high threshold of usage on a server.

Corrective controls are the remedy for errors, incidents and problems. These controls outline a repeatable method used to resolve issues and restore performance. If you have ever had to report a problem to a help desk or call technical support, you have used a corrective control.

Control Type	What it does	Example
Preventive	Stops undesired outcome from occurring.	Filling the car with gas before a long trip prevents running out of gas and becoming stranded.
Detective	Alerts when a set of predetermined conditions are met	The low fuel light on the car's dashboard alerts you to get gas soon before the car depletes its' supply.
Corrective	Reverses an undesirable outcome	Using a gas can to replenish the empty tank that has left you temporarily stranded.

So I need controls, but are all controls created equal?

Kevin Behr and Gene Kim, the authors of the Visible Ops methodology, made an important discovery. All of the high performers they had identified shared a major investment into



Change, Release, Problem and Incident management processes. But even more interesting was the closed-loop nature of these processes. By using change detection these organizations could prevent, detect and correct issues much quicker than the rest their peers. In fact, it quickly became obvious that the ability to detect changes to infrastructure formed a critical linkage between these processes.

Recently the IT Process Institute conducted important empirical research to determine which processes and controls correlated with high performance in IT. This study validates the key findings embodied in Visible Ops, and provides even more clarity around what it takes to achieve high performance in IT.

Visible Ops chronicled many lessons learned at IP Services in the course of our own process and service improvement programs. As its first adopter, we have deep experience with what it takes to be a high performer. Continually ranked in several categories as one of the highest performing IT organizations via third-party benchmarking, we have passed every external audit and SAS70, and are vigilant with our own rigorous internal control self-assessments.

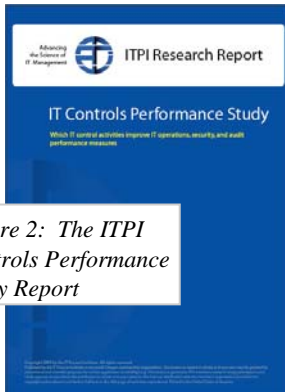


Figure 2: The ITPI Controls Performance Study Report

In the IT Controls Benchmark study,² performed by the IT Process Institute, a high correlation was discovered between organizations with the ability to monitor and detect change on their infrastructure and configurations, and their overall performance.

Where risk is greatest, these controls work best in combination. Access control is a great example of a preventive control as it does not allow anyone without prior authorization access to infrastructure. Incident and Problem management are examples of corrective controls. These processes are responsible to repair or restore what breaks to a working state.

It is one thing to have a change management process in place. It is quite another to enforce it with the use of a detective control! This ability to automatically detect change combined with a clear and enforced policy forbidding unauthorized change is a discriminating factor separating high performers from everyone else. This change detection capability is often extended and integrated into incident and problem management processes. These organizations know that not only are most outages the results of changes, but that eighty percent of the time it takes to resolve many issues is spent determining just what changed.

Since changes to infrastructure account for such a large percentage of outages, the coupling of rigorous change testing, approval and management increases the likelihood that the activities performed will be successful. Many IT operations do not even measure their change success rate, let alone design systems of control to regulate and improve it.

The benefits of change management and detection are two-fold. By eliminating risky changes there are fewer incidents resulting in outages. Secondly, when working an incident or problem, the faster change can be ruled out as a causal factor, the less time it takes to resolve

² More information about the study can be found here:
http://www.itpi.org/home/controls_benchmark.php

an issue. High performers triage problems in the order of their statistical likelihood of causation. This is yet another reason why high performers enjoy better uptime metrics as well as lower mean-time-to-repair.

How we extend our proven controls to your environment

When evaluating a service-providers' ability to service and control your infrastructure, look for an integrated service management suite that you can interact with. This suite should allow you portal-style access to service tickets, change requests, work packages, and change detection information. It is very important that your staff is not only aware of, but actually participates in the change, incident and problem management activities that govern your infrastructure.

It is vital that your team not only submit tickets for all requested changes, but that your team participates in regular, structured change management meetings with your provider. These meetings can be driven internally or by the service provider. If you have an established change management process, find out if your provider will embrace it. And more importantly whether they will work with you and integrate it in to their governance approach. If not run, don't walk away and find a provider that understands this critical success factor.

Successful Change Management is the only major key to the reliability of your infrastructure. Although, it is proven that you will have little chance achieving your goals without it. Also proven is the value of an automated set of tools supporting workflow, notification and health reporting around your infrastructure. This automation enables critical integration with your internal processes and controls.

Key attributes of high performers you will want to look for in a provider

Can they control your infrastructure by controlling who has access to it? It is crucial for a service provider to have tight access controls in place. In fact, this preventive control can pick up where other processes may leave slack. If you can't get to the server without change management approval, unauthorized changes are less likely to occur. Ask to see sample access logs. Make sure you understand how they apply to the specific architecture you are looking to have the provider manage.

Are there consequences for unauthorized change? In the event that an unauthorized change occurs, what is the policy of the provider? How many unauthorized changes can their employees make before corrective action is taken? This may sound draconian, but this type of behavior is the equivalent of not being able to balance your cash drawer at a department store. Once is quite enough. Three times is a disaster and usually means it is time to look for another, less critical position in the company or quite possibly another job.

Can the provider extend their tools and processes to you? At IP Services we have built a strong culture of causality and change management that is truly pervasive throughout our IT operations. Better than just building world-class processes for ourselves we have literally extended our own processes and made them available to our clients!



Over the years we have invested considerably in automation of our world-class processes and controls. This required not only the selection of best-of-breed applications such as Tripwire Enterprise, but also in costly customization and integration between these applications. The result is truly impressive. We have codified and automated our Change, Incident, Problem and work request management methodologies and built them all in to a solution called Interchange.

IP Services' Interchange suite was originally designed for our own network operations center and data center engineers. Many of our larger clients asked us if we could extend the application to cover their processes and infrastructure within our datacenters. Buying, learning and configuring all of the commercial applications necessary to run key processes is not only time consuming, it is very expensive. Even if you were able to get everything working on your own, the task of integration of all of the applications is a serious undertaking.

After much praise from our clients, we started to get requests to extend Interchange outside of our datacenters and make it available to them to use in their own IT operations. Many wanted to run their internal Change Management process with our workflow-driven approach. Others wanted the ability to extend our fully integrated change-detection capabilities, powered by Tripwire Enterprise, into their own datacenters and remote office environments. These requests, coupled with the desire to bring all infrastructure management under one roof, so to speak, drove new revisions and applications for Interchange.

No longer do you have to source, buy, install, configure, integrate and train your staff to operate software to manage your IT operations. Interchange allows you to start managing your IT operation in weeks instead of months. Our best-in-class process flows are already built-in. We have already integrated the processes with critical controls. You can simply subscribe to the results of our huge investment.

Interchange already has everything built in and ready to go! Take advantage of our world-class process flows and fully integrated Change, Configuration Management Database, Incident and Problem Management. Interchange is preconfigured to handle these process workflows.

We can manage your infrastructure here, there, or anywhere

Not every IT asset needs to be co-located in a hardened datacenter to benefit from IP Services' management processes and controls.

Yes, you read correctly, this is not only possible, but for some infrastructure it makes great sense fiscally to have it remotely managed.

There are critical components to your network such as routers, switches, files servers and intranet services that can not be moved from your company's physical locations. Also, many enterprises have QA environments used to test new applications and moving them offsite is not practical. Furthermore, critical pieces of IT infrastructure that form the underpinning of many critical internal applications such as DNS, content filtering, Active Directory and single sign on services are best housed close to the user population.

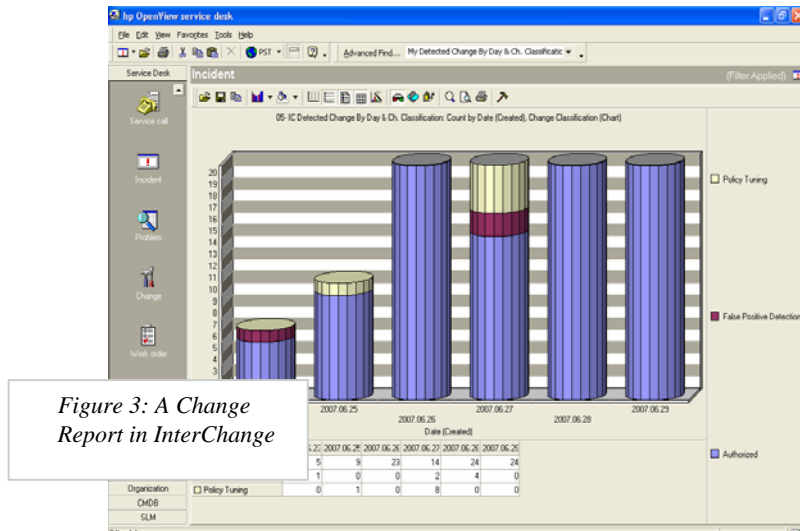


Figure 3: A Change Report in InterChange

IP Services can seamlessly manage your infrastructure whether it is located in one of our datacenters or in your remote offices. When we manage your infrastructure we extend our world class tools and processes to you. You can experience the peace of mind that your infrastructure is being cared for and monitored correctly by participating in our robust change management processes. See what work packages and service requests are being performed, and when, simply by logging in. You can not only view the work they have been assigned, but interact with Network

Operations staff members via Interchange. You can also manage the infrastructure that you govern locally in the same application. Imagine one seamless view of all critical IT assets and their dependencies.

By extending our change detection, process workflow, and critical controls to you, we can free up internal resources and increase the reliability of your applications. Gone are the days that running down router or other infrastructure issues consume hours and even days of your precious time. By leveraging the same world class staff, processes, and controls we use in our datacenters, you can enjoy the security, uptime, and performance you get from your hosted infrastructure, right at your desk!

Bring it all together to get the best results

When it comes to reliability, choose a provider that brings it all together: People, process, and technology. Our datacenters are extremely hardened and robust - biometric access control, video surveillance, electronic rack access control, redundant routing, extremely scalable tier one bandwidth, power and HVAC options - coupled with radically superior process and controls, produce better results than mere physical redundancy alone.

Combine this with our thought-leading staff and an audit-proven industry-leading system of internal controls with amazing purpose-architected infrastructure and you have the IP Services reliability advantage. Experience for yourself what tomorrow's software, security and best practice leaders already enjoy...our rock solid service here, there or just about anywhere. Contact an IP Services sales engineer today to find out what our unique approach can do for your bottom-line!