

White Paper:

## Maintaining Control in the New "Atomic IT" Environment



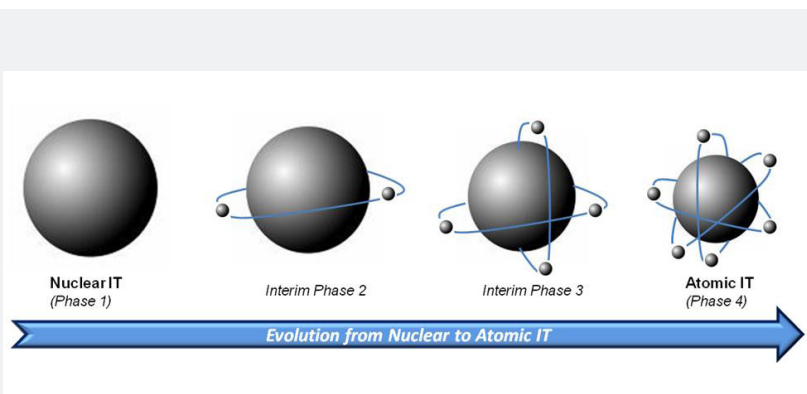
Michael Kerman, Director of IT Solutions  
 CDI IT Solutions  
 (215) 282-8738

**Across all industries and company sizes, IT organizations are facing cost, agility and service level pressures that are driving them to truly transform and not just evolve. Unlike previous computing eras that were led by either overhauling applications or infrastructure, intense pressures are causing a new era to emerge - the era of Atomic IT™.**

The move to an Atomic IT model certainly addresses many of the current concerns of IT executives including the high fixed cost of data centers, risks of in-house application development, costs and complexity of managing and maintaining legacy applications, and more. However, while this change will cause some traditional headaches to diminish or even vanish, new challenges will emerge. This paper outlines how the shift to an Atomic IT model will impact IT organizations and what steps they can begin taking to mitigate these new-age risks and costs.

### Understanding Atomic IT™

Before we can understand the challenges of the Atomic IT model, the concept needs to be explained. To begin, we need to think of IT Management in several waves, as shown below.



In the traditional Nuclear IT model (Phase 1), everything is owned, managed and delivered by the Corporate IT department, with most of the resources and assets behind

corporate walls. For many years (or even decades) this was the dominant approach. However, as distributed and web-based computing grew, complexity skyrocketed and so did the fixed cost of IT operations. This forced many IT departments

*"Just as electrons are controlled by the configuration of the nucleus, such is the case in Atomic IT where the external operations and services exist and are controlled by the core IT operations."*

to the breaking-point and so an interim, unstable era emerged, Phase 2. In this model, IT began to look outside the walls for help. Specialty applications such as Payroll, Time Management, Sales Automation and certain IT operations (including help desk) began to be outsourced simply to prevent the IT organization from collapsing. Although the results of outsourcing were not uniform, IT organizations realized that they could operate more efficiently by moving some projects and functions outside their walls and managing them via service level agreements (SLAs). Just as electrons are controlled by the configuration of the nucleus, such is the case in Atomic IT where the external operations and services exist and are controlled by the core IT operations.

As outsourcing became more capable, proven and commonplace, IT organizations began to evolve into Phase 3. This is where we believe most corporate IT organizations are today. They are supporting a wide range of users and technologies and still have a stronghold on critical corporate assets such as the data center, data, risk and compliance issues, etc. However, these organizations have built (or are building) an ecosystem of application, infrastructure and service partners to assist them with non-core work (e.g. archival, disaster recovery, data cleansing, etc.) as well as core applications (e.g. CRM, Sales Force Automation, ERP). It is during this Phase 3 that we are seeing the IT organizations becoming smitten with the potential economic benefits of Software-as-a-Service (SaaS).

While we are seeing companies willing to relinquish some control over applications in Phase 3, they still are holding

tight to their hardware. We believe Phase 4 is where this transformation becomes “complete”. Phase 4 represents the mass adoption of SaaS, cloud computing and virtualization, all of which enables IT organizations to radically change how they deliver computing services to their end users. This is Atomic IT. The table below summarizes the different attributes of Phases 1-4.

	Phase 1 – Nuclear IT	Phase 2	Phase 3	Phase 4 – Atomic IT
<b>Users</b>	Mostly employees	Employees + Partners	Employees, Partners, Customers	All relevant stakeholders
<b>What IT Owns</b>	Everything; hardware, data applications, policies, risk, etc.	Everything; hardware, data most applications, policies, risk, etc.	Data centers, some applications, SLAs, risk, data, compliance	Data, Business Intelligence, Risk, Compliance, Specialty Apps
<b>What IT Doesn't Own</b>	Very little; specialty applications	Help desk, specialty applications	DR/BC sites, data archival, SaaS-based applications	Data center, DR/BC, most applications, storage, etc.
<b>Cost Structure</b>	High Fixed Cost	Very High Fixed Cost	Moderate Fixed Cost	Low Fixed Cost

Atomic IT is a fundamentally different operating model for the IT organization. The core becomes smaller in size, with more services and operations being delivered externally. As the core becomes smaller, it undergoes a considerable metamorphosis although its importance in keeping the “atom” together remains unquestioned. Instead of doing most of the work, the core is responsible for managing, directing and monitoring the myriad of partners who are doing the work cheaper, faster and more efficiently. By offloading and “renting-back” computing power, storage and application usage, IT organizations can convert high fixed costs into variable cost, enabling more flexibility as the business changes. Additionally, patching and maintaining both current and legacy applications, DR/BC and other labor-intensive tasks can usually be performed less expensively by IT service partners. This results in lower fixed cost, less hardware and applications to manage and greater agility. So where’s the catch?

### The Challenges of Atomic IT

Recently, I met with the CIO of a large energy company. In reviewing his organization, I was amazed at how many different aspects of the IT environment had been outsourced.

Servers, networks, data warehouses, sales applications, customer service - the list went on. The CIO explained that he needed to re-tool his team. His current team was comprised of technology-savvy “do’ers”. However, in his outsourced model where partners perform much of the execution, he still needed a core group of IT-savvy professionals who were experts in contracts, service level agreements, process optimization and governance. In short, he needed a team that could:

- Establish and monitor service levels
- Track, prioritize and escalate issues regarding third-party IT services providers
- Perform Independent Validation and Verification (IV&V)
- Ensure data security

It is quite evident that the skills and resources that have brought organizations to Nuclear IT are not going to be the same as those critical to evolving to Atomic IT. Just as many companies needed to re-tool as they evolved from building custom applications to purchasing “commercial, off-the-shelf” (COTS) applications, so too will they need to retool for this next wave of IT management.

### Establishing and Monitoring Service Levels

Managing delivery of services by an external partner generally requires more formal agreements such as Underpinning Contracts (UC), Operating Level Agreements (OLA) and/or Service Level Agreements (SLA). This represents a shift from the more informal manner in which many internal IT departments service their business users. In fact, even in organizations that utilize SLAs, the sheer fact that both the service delivery and service consumer organizations are within the same organization makes an enormous difference.

*“An SLA is part of the contract between the service consumer and service provider and formally defines the level of service. Common criteria include the availability, reliability and performance quality of delivered services.”*

— Software Engineering Institute (SEI), 2008

Therefore, IT leaders need to develop or obtain the tools and expertise needed to raise service monitoring to a more formal, objective and metrics-based process. A few basic recommendations include:

- **Use a third-party to establish a current-state “baseline”.** One of the first questions that will be asked when transitioning to an external IT provider is “How does it compare to the way we used to do it”. The only way to accomplish this is to obtain an impartial, objective measure of the current state of service delivery. By conducting group and/or one-on-one interviews, as well as reviewing existing documentation, a consulting firm can provide an accurate picture regarding the effectiveness of current service delivery and the level of end user satisfaction.

*“Any organization moving down the Atomic IT path should significantly upgrade their service management capabilities to support their changing IT model.”*

- **Understand industry best practices.** In addition to understanding the current state of service delivery, we encourage clients to understand what the industry’s best practitioners are experiencing in terms of key service level metrics. This is essential for being able to negotiate fair rates with external service providers.
- **Employ a “discovery” phase.** Even with benchmark data, establishing a service level as well as any penalties for non-compliance or rebates for over-achievement is very challenging. Adding to the difficulty is the difference in perspective between the client and the provider. Generally, the client wants to immediately implement an SLA so they feel protected. However, the service provider is usually extremely reluctant to agree to an SLA on Day 1. We suggest a “discovery” phase of two to three months to enable both sides to jointly work out any “kinks” that surface without the fear/panic of the overarching SLA. The simple fact that an SLA will be developed in 60-90 days is usually enough of a motivator to get both teams aligned. This also sends a message to both parties of trust, collaboration and teamwork.

### Managing Issues with Third-Party Providers

Many organizations, both large and small, have struggled for years with maintaining a consistent, high-quality and metrics-based approach to handling end user computer issues. Companies using traditional “help desk” solutions have found their capabilities dwarfed by changes and growth in the business and as a result, first-call resolution rates, IT productivity and end user satisfaction all plummet.

The situation doesn’t change much in terms of managing issues with third-party service providers. In fact, since

formal SLAs will be in place, being able to rapidly resolve and accurately track incidents becomes more important than ever. Therefore, any organization moving down the Atomic IT path should significantly upgrade their service management capabilities to support their changing IT model.

While there are many ways to enhance these capabilities, using the Information Technical Infrastructure Library (ITIL) model as well as principles from HDI are the most common frameworks used. More specifically, organizations must become proficient in:

- **Monitoring.** The most basic competency required is to be able monitor both the client and third-party provider environment for end user issues or incidents. Ideally, this is both reactive (i.e. a system where users can enter and track service issues) as well as proactive (scanning the infrastructure for warning signs of availability, performance and/or service issues).
- **Prioritization.** Without an effective prioritization mechanism, even small organizations can be overwhelmed with volumes of service requests the same way network operations centers (NOCs) experience “alert storms” when the networks or servers fail. Prioritization can be as simple or complex as an organization needs, all that is important is that there is a consistent way to evaluate and categorize service issues and that this is shared with the third-party providers to ensure a “no-surprises” working relationship.



- **Escalation.** Escalating problems within the confines of a traditional IT organization isn't always easy; managing escalations and problem management across two heterogeneous organizations is even more challenging. Adopting a service framework such as ITIL can be invaluable in helping to define and implement the proper service desk technologies, processes and governance.

*"The primary objective of an Independent Verification and Validation (IV&V) engagement is to provide an objective assessment of products and processes throughout the project life cycle."*

- **Remediation.** Once issues have been identified and prioritized, they need to be resolved or a workaround needs to be developed, communicated and deployed. Some organizations make the mistake in believing that remediation is simply how quickly you get a fix/patch out to end users. This approach often fixes one problem but creates dozens more, sometimes even resulting in infrastructure and/or application downtime. Instead, organizations should expect third-party providers to leverage proven and formal change management, release management and deployment readiness processes to minimize the risk of service interruptions.
- **Analysis.** Most organizations have yet to adopt a truly metrics-drive, continuous process approach to service management. When an incident is resolved, they simply move on to the next one. However, metrics and analytics are essential to successfully moving to an Atomic IT model. Unfortunately, many traditional and entry-level help desk solutions simply lack the analytical capabilities, rendering them ineffective for supporting an Atomic IT model. Clients and their providers need a shared commitment to root-cause analysis and continuous improvement in service delivery and must ensure their service desk and related tools and processes can support the increasing analytical workload.

#### **IV&V: The "Trust and Verify" Approach**

According to the IEEE, Verification and Validation (V&V) is a systems engineering discipline that helps a development organization build quality into the software during the software life cycle. Validation focuses on checking that the software meets the user's needs (i.e. "doing the right thing"), and Verification confirms that the system is well

engineered (i.e. "doing it right"). The primary objective of an Independent Verification and Validation (IV&V) engagement is to provide an objective assessment of products and processes throughout the project life cycle.

This principle can be applied to any IT project, not just software development. In most cases, it is best delivered by an organization that is technically, managerially and financially independent of the IT project. Some organizations use internal Audit/Program Office teams to perform IV&V while other clients use third-party IT services firms to provide the services on a regular basis. These services often include:

- Criticality Analysis
- Requirements Analysis
- Requirements Tracing
- Milestone Reviews
- Software Design Analysis
- Metrics
- Test Witnessing
- Test Planning, Execution & Reporting
- Training Evaluation
- Site Acceptance Testing
- Defect Investigation
- Independent Assessments
- Code Analysis
- Document Inspection

In an Atomic IT model, IV&V plays an important role in helping to educate the project management teams at both the client and third-party providers on industry best practices for specific tasks or phases. It also provides an escalation path for issues and obstacles of project's success. IV&V facilitates early detection and correction of errors, enhances management insight into risks and ensures compliance with project performance, schedule and budget requirements. As an example, the State of Georgia made a \$2.1M investment in formal IV&V services and realized savings in excess of \$29M. These processes achieved the following:

- Improved early detection of problems
- Provided early escalation and recommendations
- Averted potentially fatal problems during procurement and execution
- Provided improvements in final phases of delivery and transition, averting costly testing and roll-out problems

### Ensuring Data Security

A long time ago, data resided in the data center and on desktops but was virtually always within the corporate IT boundaries. In an Atomic IT model, those boundaries are blurred even more than they are today. Conducting business and supporting real time transactions in a highly-distributed Atomic IT model means data is shared among an increasing number of IT partners. This begs an extremely important question - "Are your IT partners protecting your data as well as your company is?"

*"A total of 225 breaches of patient health information have occurred since the interim final rule on breach notifications was issued in Aug. 2009 as part of the HITECH Act. These breaches impacted more than 6 million individuals and 61 percent of breaches stem from malicious intent."*

— Beckers Hospital Review, February 2011

Organizations moving along the Atomic IT continuum should seriously consider adopting a framework for assessing and managing the risk associated with sharing information with IT partners. There are a multitude of standards and frameworks such as Shared Assessments, CoBIT, PCI or ISO27002, many of which have origins in highly-regulated industries such as Financial Services, Banking and Healthcare. Unfortunately, many organizations find these frameworks to be extremely complex and too taxing and invasive for many of their IT partners. Fortunately, there are firms that specialize in designing, implementing and managing the security assessments of IT service providers. This helps eliminate a client's need to build this capability in-house, actually, it is much like a "security-specific" IV&V service, as mentioned above.

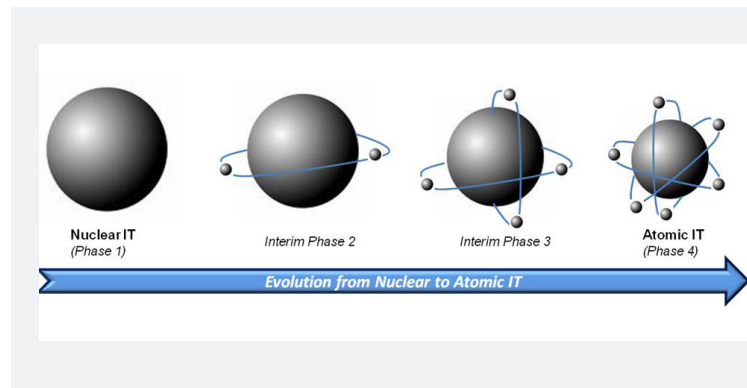
Service Provider Assessments should cover all aspects of data security including:

- Security Policy
- Logical Access Control
- Incident Response
- Foreign Vendors
- Asset Management
- Change Control
- Systems Development & Monitoring
- Disaster Recovery
- Business Continuity
- Regulatory Requirements

- Desktop
- Email & IM
- Communications & Connectivity
- Application Security
- Encryption
- Physical Security
- Media/Vital Records
- Standard Builds
- Data Integrity (at rest, in motion and archived)
- Website

### The Future of Managed IT

The direction is clear; all organizations are moving along the Atomic IT continuum. In fact, the changes in end user needs and customer demands as well as advances in messaging, mobility and cloud-based IT services represents an insurmountable force. Organizations that fail to acknowledge and adapt to these trends will be at a significant and potentially terminal competitive disadvantage.



So, the question needs to shift from "do we want to move this way" to "how do we evolve and still maintain adequate visibility, controls and accountability?" We believe that organizations should invest in these four IT management disciplines to minimize the cost, risk and disruption associated with this evolution:

- Establishing and monitoring service levels
- Managing issues regarding third-party IT services providers
- Performing Independent Validation and Verification (IV&V).
- Ensuring data security

The benefits of a more nimble, cost-effective and scalable IT organization await!

To learn more visit: [www.cdi-its.com](http://www.cdi-its.com)