EDPACS: The EDP Audit, Control, and Security Newsletter

Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/uedp20

Governance in the Cloud

Marc Vael

Published online: 17 Jul 2013.

To cite this article: Marc Vael (2013) Governance in the Cloud, EDPACS: The EDP Audit, Control, and Security Newsletter, 48:2, 7-12, DOI: 10.1080/07366981.2013.803870

To link to this article: http://dx.doi.org/10.1080/07366981.2013.803870

GOVERNANCE IN THE CLOUD

MARC VAEL

Abstract. As cloud computing has proliferated, two main problems have occurred: IT has been kept out of the loop or brought in but perceived as a bottleneck. This article examines how governance can solve both of those issues and increase the business value of the cloud.

For many organizations, cloud deployment has grown organically over the past few years—and, as a consequence, has led to a situation where many cloud deployments are perceived as "the wild west." Root causes for how this arises vary of course, but one common way is due to adoption driven by areas outside IT that have not historically been directly involved in technology acquisition. It's hard to get concrete numbers of exactly how prevalent this is, but recent research from Forrester estimates that for every cloud use case that the CIO knows about, there are between three and six that they do not,[1] suggesting that this happens more frequently than not.

This situation arises for a number of reasons: it can happen when business leaders see IT as a bottleneck and feel that their department personnel can implement faster themselves. It might also happen more innocuously—for example, when they do not realize a particular purchase is "technology" *per se* (e.g., when they adopt an as-a-service cloud-based application). Other times, it can be a matter of survival: when they face business problems so pressing that adoption now versus two months from now (e.g., when IT has bandwidth to accommodate their request) could very well mean the difference between success and failure of their product line.

But regardless of *why* this happens, the fact *that* it happens can ultimately become problematic. Each individual deployment might seem not only innocuous, but beneficial. However, over the long-term and in aggregate, lack of oversight can introduce "drag" on the organization in unexpected ways. Like barnacles on a ship, the effect of one might go unnoticed—but hundreds or thousands will, without fail, slow the vessel down.

WHY MATURE CLOUD CAUSES DRAG

It is important to first understand these detrimental impacts, specifically how and why they occur. As cloud matures within an organization, three things happen: first, individual implementations tend to grow in scale and scope. Meaning, a relatively simple deployment tends to expand as new capabilities are introduced, as

usage proliferates, and as integration with other systems occurs. For example, something like an as-a-service expense reimbursement system might start off fairly simply—but as it is used, pressure will increase to integrate: for example, to collect data from back-end Human Resources databases, to integrate workflow-driven approvals, to interface with time tracking systems, and so on. So while any given deployment starts simply, chances are low that it will stay that way over time.

Second, while each individual deployment is growing in complexity, so is cloud usage generally. Without oversight and planning, redundant and overlapping implementations proliferate. For example, the inside sales team might be evaluating and deploying as-a-service lead tracking systems at exactly the same time that the channel sales team is planning its own. The end result: the same capability is implemented two different places by two different vendors. Enterprises are far enough into the adoption curve to see this in action: data from *Information Week* Analytics' *2012 State of Cloud Computing* report[2] suggests that, of organizations using cloud computing, only 27% employ a single provider. The rest use at least two, with some using as many as 10 or more.

It is clear that complexity is increasing both locally (as it pertains to each individual usage) and in aggregate. This is where drag comes in. In a single, small deployment there is relatively little friction with other systems; since benefits are immediate (as they typically are brought in to revolutionize some slower, less efficient process), the implementation is perceived as a win. Over time, though, when deployments get larger and start to interact with other areas, they start to weigh things down: proliferating service provider relationships obviate volume pricing, lack of standardization makes future integration efforts more difficult, and overall risk to the organization is increased. Paradoxically, this undermines many of the benefits that drove cloud adoption in the first place: what started with the intent of cutting costs, increasing efficiency and fostering agility could wind up costing more, hindering business and reducing efficiency.

Finally, based on the (lack of) success of the use of its solutions, the cloud service provider might change its business approach, making it more expensive, or more complex or more time-consuming to use the proposed solution. This also can cause "drag" within the organization, which is using these solutions almost as a utility, meaning it is always available wherever and whenever they want.

This is why governance becomes increasingly more important the more mature—and more widespread—that cloud usage becomes. Recall that the ultimate point of technology governance is about business goals: policies ensure consistent usage within defined parameters, systematic measuring capabilities help the business understand return on investment, and risk management helps put technology problem sources in context so they can be assessed holistically and addressed systematically.

THE FUNDAMENTALS

Assuming enterprises want to do this, how should they start? A useful first step, before starting in earnest to make

modifications to anything directly (either to the technology or how it is governed), is to establish visibility—both from senior executives and board members and among peer organizations. Visibility from above means that those who have the widest view (i.e., the C-suite and board of directors) understand and agree with the value of cloud and the return it provides. The point here is not to get them to understand the nitty-gritty of how cloud works, but instead to give them a chance to align the use of cloud computing with organizational goals. ISACA's recent white paper,[3] "Cloud Governance: Questions Boards of Directors Need to Ask" summarizes the intended outcome here succinctly: "To establish a clear direction that is aligned with enterprise strategy, members of the board need to have a clear understanding of cloud computing benefits and how to maximize them through effective end-to-end governance practices." The focus at this level should be on the benefits and on how to maximize them.

In addition to awareness from the executive team, it is also helpful to conduct outreach to the stakeholders themselves (such as the business and technology communities). Why? Because sometimes even the word "governance" scares people. Areas of the business that need to be agile and react quickly sometimes feel that oversight equates to slow. If they feel that oversight is going to slow them down, they might try to go around it and stay with business-as-usual adoption patterns. As a consequence, it is important to clear up any misconceptions and nip the "slow" perception in the bud early.

Start with candid discussions with stakeholders about what the enterprise is trying to do. Stress that the point of governance is to allow maximum return on investments already made, and not about extra management or unnecessary overhead. One way to approach this is through the use of COBIT 5[4] principles and enablers as a context for that discussion. Speaking directly to the principles is a good way to get stakeholders on board. Specifically, seeing that "meeting their needs" is one of the core principles of the entire activity (in fact, it is number one) and that "separation of governance from management" is a key tenet (number five) can go a long way to engendering their support and reducing anxiety. From there, introduce principle three and speak to why end-to-end coverage is important and how existing deployment characteristics may not be helping to support that precept.

Build on that through discussion of the enablers, discussing frankly with them how resources and principles/policies/frameworks work in tandem to the betterment of both (because ultimately this is the goal). It is always helpful to see this in context, so have available or prepare a business case that highlights this and shows them concretely why the current environment creates challenges and how agility and efficiency are slowed, rather than increased, by virtue of the current situation. By doing this, stakeholders who might have reacted negatively to more structure might actually help bring it about instead.

EXPANDING EXISTING GOVERNANCE STRUCTURES

Once (most) everyone is on the same side, it is important to understand the technology governance process already in use. This is because (trite though it sounds), the ultimate goal is not to create something new (which, in itself, represents significant investment), but instead to adapt what is already there to cloud technologies. If there is not already a structured governance methodology in place (as might be the case in a relatively new organization), cloud might provide the impetus for a broader, more comprehensive effort. In that case, a framework for enterprise governance of IT (such as COBIT 5), might be something appropriate to consider at this point. It is important, though, not to *just* address cloud in isolation in doing that. Instead, it is critical to recognize that cloud is part of a larger technology portfolio and needs to be addressed within that context.

If the organization already employs a systematic governance approach, the onus will be on making two things happen: first, expanding those structures and modifying them if needed to address cloud, and second, championing the governance methodology to make sure that individual lines of business work within it rather than around it. This will help uncover and ultimately feed in specific use cases that might not be anticipated if operating in a vacuum.

In terms of incorporating cloud into the existing governance approach, it is important to recognize where what is in place already might not be a clean fit—for example, where supporting policies, and the processes/procedures that enforce them, might not address cloud or address it poorly.

Consider an organization that requires all technology projects above a certain financial amount to go through a review and approval process. The point of this, when it was initially set up, was probably to establish a consistent process such that redundant or overlapping usage can be identified, to better negotiate volume pricing, to analyze risks prior to deployment, and so on. But how would a pay-as-you-go approach fit into that model? If the situation starts free or very small price-wise and grows from there, the organization could be very far down the adoption pathway before it hits anybody's radar. Does that address the original goal for which the process was set up? No, because the organization in a pay-as-you-go cloud situation would be committed before there is time to preemptively act. This type of framework works well in a traditional IT context, but may not work well for cloud. The same might be true of other policies—or even other artifacts of governance, such as measurement, return on investment (ROI) calculations and risk analysis. Each aspect of the governance model should be viewed critically to determine if the original intent is being satisfied.

If this sounds like it is a lot of work and hard to accomplish as one person, that's because it is. Working directly with stakeholders early and getting their buy-in is critical. Ultimately, the degree to which efforts can be governed successfully will depend on the degree that the team can discover, incorporate, and adapt to unforeseen use cases. This is because there is a near-infinite

landscape of use cases to which cloud could apply—more than any one person, one group, or one point in time can identify and address. For example, a developer using Amazon EC2 to test an in-house app is "cloud" (public infrastructure as a service [IaaS]), an IT group building an in-house virtualized data center might be "cloud," depending on implementation and the definition applied (private cloud), and a remotely hosted application is also "cloud" (software as a service [SaaS]). If these sound wildly different, that is because they are. Trying to pigeonhole the usage is counterproductive.

Instead, gaining the support of others is critical. Establish a feedback loop where stakeholders share what they are doing, why, and what benefits they hope to realize. Be especially receptive to situations where current governance structures do not work or obviate the benefits stakeholders expect to realize; work together with them on finding a way that they can do what they want within the existing structures rather than going around them. Recognize, though, that compromise cuts both ways: adjustments to governance structures themselves may be needed in order to meet stakeholder needs. This implies that the governance model needs to be *at least as agile as the business dynamics being supported*. So if a particular usage cannot fit in cleanly, the answer cannot be "hold on while I take a year to update the framework." If it is, they will find a work-around.

Teams will discover as they do this that this process is most effective when it is iterative—that is, when it's a process of continuous refinement and improvement as new use cases are discovered and the structures are adapted as a result. It is best to cultivate a track record of adding value to stakeholder efforts (or, at a minimum, not subtracting from it) to make this feedback loop viable. A failure early when the team is establishing credibility could mean they do not come to team members next time; adding value means they will continue to support the effort and come back with information about what they are doing next time.

The meta-point is that existing governance frameworks can be used effectively to address cloud, although successfully doing so requires joint participation and some degree of flexibility in how they are applied.

Notes

1. http://blogs.forrester.com/james_staten/11-10-25-what_are_enterprises_really_doing_in_the_cloud
2. http://reports.informationweek.com/abstract/5/8658/Cloud-Computing/research-2012-state-of-cloud-computing.html?cid=pub_analyt__iwk_20120206
3. ISACA, "Cloud Governance: Questions Boards of Directors Need to Ask," 2013. www.isaca.org/cloud-governance
4. ISACA, "COBIT 5: A Business Framework for the Governance and Management of Enterprise IT," 2012. www.isaca.org/cobit

Marc Vael, CISA, CISM, CGEIT, CRISC, CISSP, ITIL, is international vice president of ISACA and chair of the association's Knowledge Board. He is also chief audit executive at Smals, in Belgium. He can be reached at marc@vael.net.