The arrival of cloud has shaken up many IT departments and long-held ways of doing business have been shoved aside. For example, the idea that business expansion could only occur by provisioning new servers has all but disappeared. Even more radically, the notion that IT departments are solely in charge of buying software has also stepped to one side. Indeed, business departments are assessing and even purchasing applications, and that’s a situation that is not going away any time soon.

Cloud touches every aspect of a business. This can be demonstrated by the way that it impacts on data governance. The arrival of a cloud provider changes everything. If you look at the definition of data governance from the Data Governance Institute (DGI), you can see where some of the sticking points are: “Data Governance is a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods.”

There are some obvious hot points here: “accountabilities” and “who can take what actions” are areas where meanings can be interpreted very differently.

Data governance is a big problem for CIOs, particularly people who have been a long time in the industry, ones who started off as more akin to CTOs looking after hardware and wires. They don’t really understand the business issues.

Data governance in the cloud

Moving to the cloud has plenty of implications for the way that data governance is handled within organisations. How should firms approach this?
Data governance in the cloud

Business issue
According to HP fellow Mateen Greenway, there’s a more fundamental problem. It’s one that’s to do with the way that CIOs operate. “Data governance is a big problem for CIOs, particularly people who have been a long time in the industry, ones who started off as more akin to CTOs looking after hardware and wires. They don’t really understand the business issues,” he says.

In this world where lines of business have a big impact on the way that software is chosen, this can really matter. CIO thinking has to change, according to Greenway. “They’re still thinking in bits. They need to start thinking at the opposite end. ‘Who are the people who want this information and who gets value from it?’ Data governance becomes how to meet that need too,” he adds. “CIOs are used to worrying about the storage of data, now it needs to be about getting that data to the right people.”

There’s also the concern about what else happens to that data. Individuals have been considerably more agitated about threats to data security and privacy since the revelations by Edward Snowden that NSA agents were looking into Europeans’ data. The news made many businesses extremely jumpy about putting their data (or customer data) in multi-tenanted cloud providers.

According to Clive Longbottom, founder of analyst firm Quocirca, companies are certainly questioning who’s looking at their data — whether that be the NSA, GCHQ or whoever — but he says that much of this is overstated. “For the average company, there’s going to be little interest from the security forces. It’s only in industries like defence, petrochemical or aerospace that they’re going to be interested,” he says. “Your main worry is going to be the black hats, who certainly will be interested in things of financial value that you have.”

Trust
Trust is at the heart of the problem when it comes to moving to cloud. Do you trust your provider? It’s a problem that’s particularly acute for small businesses, as they may not have security resources on hand in-house. According to a recent survey from the University of Bournemouth, just over half (54.6 per cent) of small businesses cited data protection and privacy as the main reasons for shying away from cloud services. The ironic thing is that it is precisely these companies who would most benefit from the cloud — it’s a way to bring enterprise-class security to SMBs.

Some SMBs are worried that cloud service providers will not bring industry best practice to the table. There are also concerns that companies will not know where their data is being held. Any company that has dealings internationally or sends data across borders has such worries. All cloud users need to have an idea of national laws and regulations from the outset.

CIOs should start off by asking cloud providers some basic questions, advises Longbottom. “For a start, you should ask whether their datacentres are ISO 27001 compliant and then you should be asking them how they deal with data sovereignty: you want them to say where the data is,” he says.

Some of the low-cost providers may try to

Cloud covers a multitude of sins and you have to realise that not all cloud providers are the same: some clouds have high SLAs, some have none. You can only select the right tool if you understand the needs. For example, you wouldn’t treat a Porsche and a truck the same. The Porsche has a lot going for it, but you can’t deliver a piano with a Porsche."
blur the issue of where data is being held by using content delivery networks (CDNs) or wide area data accelerators but, as Longbottom explains, this is little comfort to customers. “The best service providers don’t do this – the low cost do and will shift everything to Akamai or Limelight. You have to understand that you’ll have to pay to get the best solution,” he adds.

HP’s Greenway concurs, saying: “Cloud covers a multitude of sins and you have to realise that not all cloud providers are the same: some clouds have high SLAs, some have none. You can only select the right tool if you understand the needs. For example, you wouldn’t treat a Porsche and a truck the same. The Porsche has a lot going for it, but you can’t deliver a piano with a Porsche.”

If a company has a data governance professional, it’s key that they are involved in the decision to move to the cloud from the outset. Only a data governance professional can address all the regulatory concerns: CIOs don’t have that expertise or that level of experience.

So, what should a CIO be doing? They need to make sure they address all these concerns up front, then work out what data could be stored in the cloud. Active customer data must be treated very differently from archived data, for example. Policies should be defined and then also strictly adhered to. Longbottom advises a slightly different order to proceedings, adding: “The first thing a CIO should be doing is taking a look at the existing internal infrastructure, as it’s probably pretty bad. You can’t look to external suppliers if your internal structure is a mess.” There’s an old adage that one shouldn’t outsource chaos because the end result will be chaos. It’s a similar story with data governance. Cloud won’t solve a problem if you haven’t got the principles right in the first place.