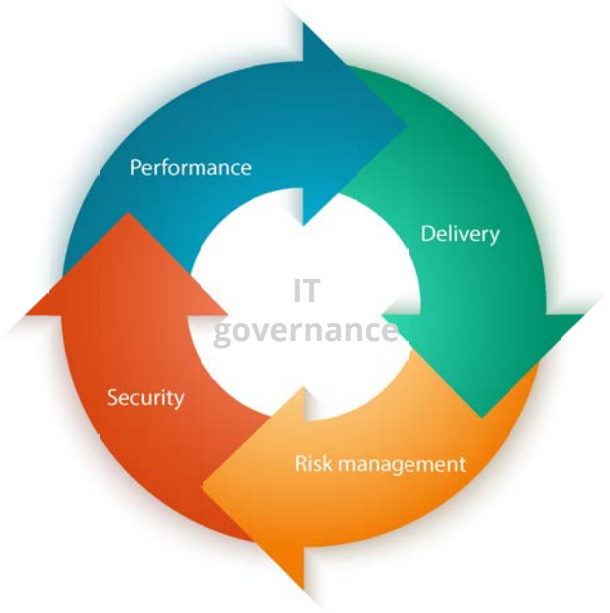
The Register®



Flexible IT governance in a changing world

More services, more choices, more than one way to get it right

---

In association with

SUNGARD® AVAILABILITY SERVICES™

Executive summary

How does IT governance respond to an increasing rate of change in the devices and services that users and managers desire? On one hand, the evidence is that untracked or uncontrolled use is fatal to governance processes. With an increased regulatory burden (not least, forthcoming EU data protection legislation), this has potentially disastrous consequences. Yet evidence from engagements is that the progress is possible.

- Often, the needs of different constituencies are not as far apart as they perceive. When IT prioritises communication, it can uncover large areas of consensus.
- Proactive IT departments can accommodate user desires (not least because ignoring them invites shadow IT).
- No improvement can happen without clarity over who runs the governance process. For functions such as security, this may not be the IT department (although it would still function as a trusted advisor). Devolving responsibility to the business may create a better environment for compliance with governance processes.

Introduction

The rate of change in IT continues to increase: there are both new services, and new ways to deliver existing services. Applications are often delivered partly on premise, partly from an external provider. Business units purchase or develop their own applications. Users bring their own devices to work, use their own services on those devices, and expect them to be integrated and supported.

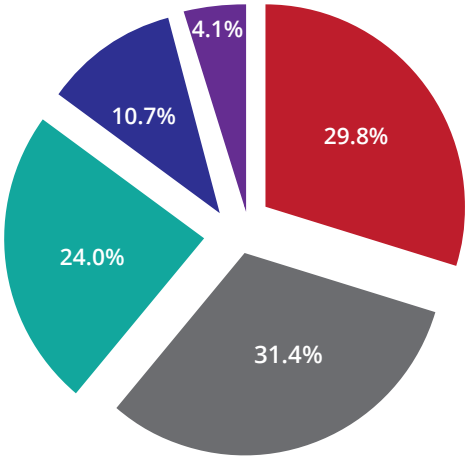
On top of this, IT provisioning and support is expected to occur in minutes and hours, not weeks or months. It is hardly surprising if, occasionally, relationships between the business and IT become adversarial: leading to negotiations that can be summarised as “if you don’t do it, we’ll find someone who can”.

The result is that, if these trends develop unchecked, it will be almost impossible to maintain coherent IT governance. Executive management rightly demands flexibility, but governance confusion is too high a price to pay, worse, it may not be apparent that this confusion exists until the business is faced with cost overruns, declining performance, or regulatory problems.

The image of the IT department as a blocker to change is, in our experience, unfounded. A survey of 121 IT professionals in 2014, found that three out of five were very open to change[1] :

Which of the following best describes your organisation?

Answer Options	Response Percent	Response Count
Flexible and agile in all our approaches and processes	29.8%	36
Open to change if the market need has been proven	31.4%	38
Open to change, but usually behind the market	24.0%	29
Open to change, but often unable to execute	10.7%	13
Change-averse	4.1%	5
Answered question		**121**

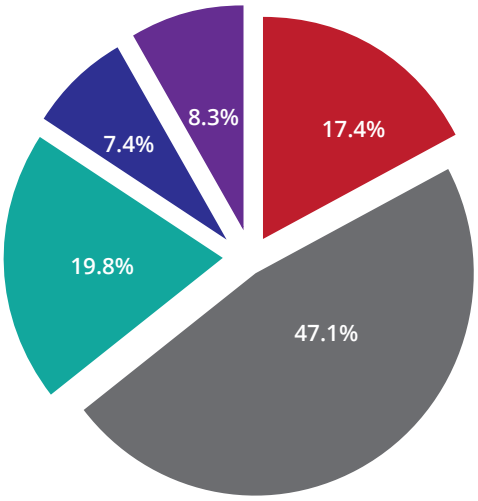


Courtesy of V3.co.uk

But this flexibility can be the cause of IT governance problems, because only one in six of the same respondents track change formally:

What processes do you have in place to manage and monitor change?

Answer Options	Response Percent	Response Count
We have systems in place to track the impact of all changes	17.4%	21
We track change on an informal basis	47.1%	57
We only assess changes regarding large projects	19.8%	24
We don't monitor any changes to the business	7.4%	9
Our business doesn't change enough to require any tracking processes	8.3%	10
Answered question		**121**



Courtesy of V3.co.uk

[1] "V3 Sungard AS Change Management Survey", V3.co.uk in association with Sungard Availability Services, September 2014.

This paper, based on conversations with businesses that have faced these problems and attempted to solve them (with varying degrees of success), examines how the IT department can become an enabler of good governance while keeping up with, or even accelerating, the pace of change.

There are many good reasons for the IT department to initiate this process, but three stand out:

- *Vision.* The IT department has the deep awareness of the transformative potential of technology across business functions, and exists to service the whole business, rather than one unit or function.
- *Capability.* The IT department can create rules and automated processes that can help implement agreed governance, and has the potential (if not always the capability today) to monitor and manage the process.
- *History.* The IT department is often considered to be responsible, by default, for governance of IT-based processes in the organisation. The IT director or CIO can use this process to clarify existing roles. Even more important, it can identify processes for which it is responsible, but over which it has no control.

Note we describe the IT department as an "enabler" of good governance. Part of this process, as we shall see, is to ideally put as much power, control and flexibility in the hands of business units and users as possible.

What is IT governance?

Effective governance involves a process of negotiation and partnership between management, users and IT in which no constituency can expect to be fully satisfied. Nor can it be defined as a set of inflexible rules, or for every business in the same way. Nevertheless, comprehensive IT governance encompasses well-defined procedures that define:

- *How you make decisions around IT services.* Which services to provide, but also who has the right to access them, and the process of negotiation.
- *How you assess user needs.* Creating clearly understood boundaries for which user wants can be satisfied, and the process of assessing competing needs.
- *How you define the services that best meet the needs.* Encompassing service levels, development, regulatory responsibilities.
- *How you make priority.* What should be done today, next week, and next year?
- *How you control how and when investments are made.* The allocation of budget and where the rights to spend that budget are located.
- *How you measure the return on those investments.* Measurable criteria for success and failure, and the process by which they are reported.

Clearly this encompasses the whole of the business, and many competing interests. It is not practical for any constituency to get everything on its wish list, but good governance also creates an environment in which constructive dialogue can take place, and compromise is possible (and respected).

Making better governance decisions

With so many competing interests, and so many dimensions to good governance, it is tempting for an IT department to shy away from attempting to improve the governanceprocess. Yet, from our experience, the interests of the competing constituencies are not as far apart as we often assume, and the business and users overwhelmingly welcome greater clarity. The perception of conflict often has more to do with a lack of day-to-day communication and collaboration than irreconcilable differences.

Achieving harmony is still a process of compromise, and so more important than the exact outcome of a governance process is the way in which decisions are reached. Governance will constantly evolve, and this is only possible if there is a basis to examine and renegotiate its effectiveness, and if the outcomes are respected and observed. Based on the experience of businesses that have embarked on formal processes to enhance IT governance, there are mechanisms by which the IT department can initiate these improvements:

1. Internally, accept the inevitability of some user desires. Business needs for mobility, for example, challenge governance because they involve supporting a variety of endpoint devices, exposing data to external networks, and may require enhancements to identity management and security. User desires are often dismissed as impractical, which is one reason why McAfee reports[2] that more than 80 per cent of them use non-approved SaaS. Yet while an unauthorised cloud service such as Dropbox might be Kryptonite to good governance, it highlights the business need that users who work outside the office will inevitably use cloud file storage, often to pass information to suppliers or partners. The same McAfee research showed that 24 per cent of users say that their unauthorised SaaS meets their needs better than IT-approved software, and 39 per cent use it precisely to bypass governance-based restrictions. Often they challenge governance because it satisfies a short-term business need: they will work better and more efficiently if compliant equivalents are available.

2. Clarify and communicate the IT strategy. If there is an overarching strategy, created with governance in mind, at both the macro (mission statement) and micro (how do we work day-to-day) level, it can be used to determine which services are priorities, and how to resolve contention over service levels. It can also demonstrate the limitations of shadow IT. For example, while three out of five users with a personal mobile device use it to access company data[3] , security problems are only one impact on governance. It also creates “islands” of information that can’t be shared easily.

2 “The Hidden Truth Behind Shadow IT”, McAfee and Frost & Sullivan, December 2013.
3 “Shadow IT in the Enterprise”, Nasuni.com, December 2012.

3. What are the regulatory boundaries, and how will they evolve? Compliance and regulation create red lines today, but feed strategic decisions. The IT department will have a better understanding of the impact of regulation on IT governance than business units. IT can create boundaries for existing services, but also act as an advisor for longer-term investment when changes in regulation can also affect which services can be planned (for example, forthcoming data protection regulation). This helps to decide where in the organisation accountability should sit, and determine spending priorities.

4. Create meaningful service measurement. Defining service quality, either for internal or customer-facing applications, in terms of narrow technical targets delivery (uptime, availability, response times) can lead to conflict if business or management perception of a service is poor, even though IT is delivering on its SLA. Defining measurements that map to the business need (transaction times, satisfaction) not only creates mutual understanding, but can also clarify the investment needed to hit operational targets.

5. Propose new ways to examine the return on investment. Governance is, at heart, a mechanism to use limited amounts of money in the best way possible. IT has an insight into this that may not be apparent to business units: for example, departmental spending may create local efficiencies, but incompatible data. Self-service and unlimited support, without any accompanying chargeback or report-back mechanism, removes incentives for business units to be careful or thrifty.

Redefining the relationship with the business

To be a catalyst in this process, the IT team must also have credibility in the business, and with individual users. To do this, there are some general principles which successful IT departments, in our experience, follow.

The first is to have as much contact with the business as possible, in a variety of ways. User surveys show that the number of touchpoints between IT and business units closely correlate with the reputation of IT inside the business. This contact can be informal, it can be reactive (support, offering consultancy, responding quickly) or proactive (training, workshops). A visible IT department can not only be seen to be in control of service delivery and management, but has the opportunity to use contacts to reinforce broader policy and principles: for example, offering help on setting security for devices is also an opportunity to explain the user's responsibilities.

A more formal approach to this is to create reciprocal representation between IT and the business: for example representatives in IT and business units to provide liaison, and to identify champions in the business to help create positive atmosphere of collaboration. This might reduce the incentive to create shadow IT, or might at least make the inevitable pockets of shadow IT visible, and so bring them into the IT governance process.

This can be expanded further, to create services in collaboration with the business, using an expanded devops team, and agile development (which, by its nature, involves continuous collaboration with the business). In this way, applications can "bake in" both user desires, and governance principles.

While governance is often thought of in the business as regulation, this process relies very much on "soft" skills and commitment: openness and a mutual commitment from both IT and the business not to become defensive can help create clear and realistic lines of reporting, and constructive dialogue to resolve governance problems. This is underpinned by the IT department's image: an IT function that is considered to be impervious to user desires undermines governance, because it encourages independent action from the business.

There is more than one way to structure this dialogue: it is common to create a process of service negotiation, in which SLAs are mutually agreed, and hopefully delivered to the business by IT. Yet successful governance often goes further. The natural outcome of the approaches above is to create a collaborative relationship, in which the IT department offers regular guidance to help shape business planning at an early stage. This can smooth negotiations, and ultimately place more responsibility for governance in the hands of the business.

An IT department that cultivates a reputation as an enabler can still deliver hard truths about the services that it can deliver: a collaborative relationship can help the business understand that flexibility and enablement comes at a cost: either a direct financial cost, or in terms of governance self-discipline.

Ultimately, this process may result in other parts of the business assuming governance responsibility for functions that have traditionally – either through design or default – been left in the hands of IT. Security and identity is one example of a function that is, at heart, not exclusively an IT responsibility, although IT can help to define and provide tools to implement security governance.

Who makes this happen?

The final point to make is that this is not primarily a bottom-up process. IT governance (or any type of governance regime) is the responsibility of executive management. The legal and operational buck stops with directors. On the positive side, this is an opportunity for executive-level leadership to use the governance process to define and accelerate change in the business: a governed policy around mobility, flexible working, BYOD or chargeback can be a springboard for operational improvement.

The result is that, instead of flexibility undermining governance, good governance creates flexibility. IT cannot do this alone: but it can lead the way to create a clear governance strategy for the delivery of its services, the IT department can be a catalyst to create a better business.

About Sungard Availability Services

Sungard Availability Services provides managed IT services, information availability consulting services, business continuity management software, and disaster recovery services. To learn more, visit www.sungardas.co.uk or call 0800 143 413

EMEA Head Office:
Unit B Heathrow Corporate Park, Green Lane, Hounslow, Middlesex TW4 6ER
+44 (0)800 143 413

Belgium
+32 (0)2 513 3618 www.sungardas.be

France
+33 (0)1 64 80 61 61 www.sungardas.fr

India
(+91) 20 673 10 400 www.sungardas.in

Ireland
+353 (0)1 467 3650 www.sungardas.ie

Luxembourg
+352 357305-1 www.sungardas.lu

Sweden
+46 (0) 8 666 32 00 www.sungardas.se

Connect with Us

twitter.com/SungardASUK

linkedin.com/company/sungard-availability-services-uk

facebook.com/SungardAS

youtube.com/SungardAvailability

blog.sungardas.co.uk