

6 BENEFITS OF GOOD IT GOVERNANCE

Organisations working from the 38500 six principles of best practice IT governance, and using a tried and tested decision-making model to evaluate business cases and to guide procurement decisions, can expect to see the following benefits:

- cost reduction;
- performance improvement;
- ability to react quickly to market changes;
- increased customer satisfaction;
- more sustainable practices;
- increased revenue per dollar cost;
- general workplace benefits for the board, management and staff.

COST REDUCTION

Cost reduction does not happen overnight. Introducing IT governance has a cost attached. However, over the course of 18 months to two years, you would expect to be able to deliver IT-enabled services at lower cost. Several factors contribute to the lower cost. Having a clearly defined strategy that is aligned with the organisation's goals and mission will enable the culling of services and systems that are no longer required. Matching capacity delivered to what is required will reduce waste – either of spare IT capacity or staff sitting around waiting for computer resources to respond.

Cost analysis of desktops and desktop support at the local university a few years ago resulted in new leased PCs being supplied to all staff and students. Previously, university staff would receive new desktops and they would pass on their old machines to their PhD students. IT desktop support staff were spending the majority of their time maintaining and repairing the old machines for the students. Replacing every desktop throughout the university freed up desktop support time for rolling out applications and supporting the teaching staff.



PERFORMANCE IMPROVEMENT

Performance improvement comes from matching performance required to performance delivered. Overdelivery of performance can be invisible and is often the result of a misunderstanding between business owners and the IT team or the work of an overenthusiastic IT team. I have witnessed highly specified, high performing IT equipment linked together with a bottleneck of a slow network. I have heard businesses demand high availability systems, when really they only wanted high availability from 9 a.m. to 5 p.m., Monday to Friday. I have seen executives issued with computers with the processing power to run the analysis for a cancer research laboratory, when really all they want is a tablet computer or large smartphone for collecting email.

Underdelivery of IT systems can also be invisible. Staff get used to slow systems and working around the inconvenience – making cups of coffee whilst their PC boots in the morning or taking notes on paper whilst on the phone to a client because the IT application cannot be relied upon to respond sufficiently quickly, or relied upon not to hang or close whilst entering data directly. Sometimes slowness is self-induced. If you have staff who have been with your organisation for over 10 years and nobody has ever spoken to them about archiving files or email, they could be forever wading through years of collateral. I have seen some amazing and worrying staff workarounds for slow or challenged IT systems.

Maybe your IT requirements are patchy and require a creative solution to turn on and turn off performance as required? Certainly the best approach is to start with your real requirements and challenge the IT delivery team to match them. Cloud-hosted systems provide the way forward for some very creative performance matching services.

ABILITY TO REACT QUICKLY TO MARKET CHANGES

One of the great benefits of having your IT housekeeping in order is that it is relatively easy to respond to market changes by reconfiguring your IT assets – whether that means a sudden increase or decrease in capacity or the addition or removal of an IT service. Also, it is relatively easy to switch on service monitoring, once you have a full understanding of which of your IT assets deliver which services. You can track usage and collect some true business intelligence data that will reveal how your customers use your services – when and why. Having an agile and adaptive IT infrastructure is not appropriate if you run a stable and static business model, but if you are trying to stay afloat and proactively deliver services in a tough business climate, then it can be the market advantage that singles you out from your peers.

Increased customer satisfaction

Although customers appreciate good service that meets their needs, they do not want or expect to pay for services that they do not want or do not use. With good governance in place you can monitor service take-up and customer response. Underproviding is often easier to pick up than overproviding, but surveys across a statistical sample of your customers should help in this respect. IT services carry high expectations – we expect the new version of the current mobile phone to be thinner with a longer battery life and more sophisticated applications, a camera to have higher resolution than the

last version and some new exciting form or feature. To constantly deliver increased customer satisfaction you need to be constantly listening to your customers to find out what improvement means to them.

Good governance practices will help you identify who is using your products and how your products are used. Once you identify a problem, it should be straightforward to work through to the root cause. Once you have identified a potential new feature, it should be easy to identify the value of the feature to customers. If it is worth proceeding to deliver the new feature, you will have the data to hand to provide accurate costing for the implementation project. Also, you will be able to provide accurate estimates for the time to deliver and the resources required. As we all will have experienced at some stage in our careers, throwing more money and more people at a project does not necessarily guarantee a faster delivery, and good governance enables you to match resources to requirements.

More sustainable practices

With a push towards sustainability and green habits, there is a greater awareness of services and their cost to the planet. This has two noticeable consequences for IT services. An IT service that replaces a paper-based system with an electronic one will be seen as good. Similarly, hardware that consumes less power or requires less air conditioning will be viewed positively.

But beware – if I provide documents to my board in electronic format only and each board member prints them out at home, then the overall cost of the delivery is higher. Similarly, if I turn down my air conditioning and run my servers in a warmer room, I am saving electricity and looking very green. However, if my servers overheat or just simply do not last as long now that I am running them hotter, then the overall saving might be negligible or non-existent.

To deliver a truly sustainable service, you need to look at the whole of life, end-to-end delivery of each service you provide.

Increased revenue per dollar cost

Good governance practices will naturally lead to a mindset of continual service improvement to drive up quality whilst making process steps more efficient and cost-effective. The Japanese practice of Gemba Kaizen uses the five Ss to drive out waste and increase quality. There are some stunning examples of massive savings in factory processes through what seem to be very minor process alterations.

The five Ss are as follows:

- **Seiri** (Sort Out) - Sort out and separate anything that is not needed.
- **Seiton** (Straighten) - Put what you need in order, so that it is ready for use when needed.
- **Seiso** (Scrub) – Prevent errors by enhancing quality.

- **Seiketsu** (Standardise) – Standardise and implement sorting, straightening and scrubbing routines.
- **Shitsuke** (Sustain) – Build sustainable practices.



Manufacturing examples are relatively easy to understand. If it takes five minutes to sew a garment and we have thousands of machinists making garments in a factory that runs 24x7, then even a saving of 10 seconds per garment can add to a substantial gain in a short period of time. There is a classic example of a quality manager making a change in a sewing factory so that material was passed to the right-hand side and not the left-hand side of each sewing machine, to save the time used by the machinist in passing the material across the machine. You would think the time saved would be negligible, but by the time the saving is multiplied by the thousands of machinists and the number of sewing slots per day, suddenly it looks like a huge saving!

Good IT governance will help you put clear IT policy, processes and procedures in place for your organisation to follow. Also, you will have IT staff who have clear instructions and the responsibility and authority to make progress on projects and to address issues as they arise. This should mean that you will avoid double-handling work and your staff will not be frustrated continually waiting for approval to proceed. Once your IT staff adopt the mindset of continual service improvement, they will be continually seeing opportunities for refining processes and procedures. One of my clients has set up a project team to deliver business improvement through the organisational IT systems. So far the team has made a number of minor but time-saving improvements. Over the course of a year these changes will save significant time and money and will provide a better and more efficient buying experience for customers.

General workplace benefits

We spend a lot of hours per week at work, and, according to psychologists, nearly all of us want to go to work to do a good job that we can feel proud about. If we provide our staff with IT systems that support their work, that are not a cause of frustration and that perform as required, we get the best out of our workforce. Moving up a layer to our managers, we want them to spend most of their time developing the business, not chasing forms. We want them to have the tools that enable them to stay connected with their staff and customers, without wearing them out with continual non-stop questions. We want them to be compliant with company policy and legislation without having to continually seek out information. IT managers need to have tools and resources to enable them to plan and procure appropriate IT support for new business developments and to plan ongoing maintenance and support tasks for operational systems. A sound IT governance framework will ensure the delivery of all the above. And, finally, we need good IT support in place for our board or governing body members – easy, but secure, access to board papers, online voting and digital signing of documents. A sound IT governance framework will provide the assurance that security has been taken into consideration when setting up systems for sharing sensitive and confidential material. Remember, though, that if you do run your board papers through the general IT systems of the organisation, your IT staff with systems administrator access will have access to them.

When an organisation is served with effective and efficient workplace systems, from the board members through to the operational and front line staff, then, generally, it is recognised as a good place to work. To test out this theory, look at your local 'best places to work' survey. Certainly in New Zealand, I can recognise a number of organisations in the 'Hall of Fame of Best Places to Work', that I know to be running efficient IT and information governance. And that brings us nicely to the final section in this chapter – what are the things that can happen when good IT governance is absent?

BAD THINGS THAT CAN HAPPEN

When you look through the list of bad things that can happen when there is no or insufficient IT governance in place, you will soon observe that these events would mostly be linked – for example, a security breach would almost always result in a reputation loss, and a reputation loss is likely to result in a loss of business. Loss of business will result in financial loss.

The reason for considering these outcomes separately is to identify the different types of governance-related root causes that can result in 'bad things':

- security breaches;
- financial loss;
- nasty surprises;
- general reputation loss;
- loss of business.

Security breaches

Security breaches fall into four main categories. A breach can be from an internal or external source and can result in the exposure or potential exposure of customer and/or organisational data. An internal breach is generally a human resources issue – somebody has used an IT system to send something to somebody who is not authorised to see it, and that somebody could be external or internal to the organisation. This is not an IT issue unless you run the type of strictly managed government agency where taking any work home can result in a prison sentence. In normal circumstances, you are not likely to set up a regime that restricts your staff from having access to anybody outside the internal staff network, as the restricted group would include all your suppliers and customers.

In contrast, an external breach is an IT issue and maybe even a privacy issue, depending on the nature of the material leaked. If somebody can break into your system and access private organisational or customer data, then you have an IT security problem. The consequences of such a breach will depend on the type of record accessed and the stakeholder group affected by the breach. Some recent examples of leaks that have made the news have included patient health records erroneously distributed via email, compact disks and USB keys containing social services data left on public transport, exposed customer credit card details and government files found to be accessible through self-service kiosks.

You might be wondering how this can be a result of bad governance. In essence, good governance policy and process will ensure that your systems are built to the required security standard. Not only that, but these systems will be audited and tested regularly to identify potential vulnerabilities. If, despite all this, a leak occurred, the organisation with good governance would have processes in place for quickly identifying the source and cause of the leak and for minimising the damage, mitigating the risks associated with the information being leaked and collecting forensic information should the event proceed to a court case.

Financial loss

The causes of financial loss through poor IT governance are many and range from user error such as an ecommerce system update that results in goods being sold at the wrong price, internal fraud and inappropriate spending on IT systems that are considerably above or below the capability required, through to poor payroll or banking systems that process transactions incorrectly. Internal fraud is more common than you might expect and, again, having good forensic practices in place is essential if you are going to be able to provide evidence of what happened that will stand up in court. And if you want to do a self-test for internal fraud on your company accounting data, and you are mathematically inclined, check out Benford's Law.



Benford's Law can recognise the probabilities of highly likely or highly unlikely frequencies of numbers in a data set. The probabilities are based on mathematical logarithms of the occurrence of digits in randomly generated numbers in large data sets. Those who are not aware of this theory and intentionally manipulate numbers (e.g. in a fraud) are susceptible to getting caught by the application of Benford's Law.

I attended a lecture by Mark Nigrini a few years ago where the theory behind the law was explained. Nigrini's research shows that Benford's Law can be used as an indicator of accounting and expenses fraud. One fraudster wrote numerous cheques to himself just below US \$100,000 (a policy and procedure threshold), causing digits 7, 8 and 9 to have aberrant percentages of actual occurrence in a Benford's Law analysis. Digital analysis using Benford's Law was also used as evidence of voter fraud in the 2009 Iranian election. Nigrini demonstrated how Benford's Law could be applied to the accounts of companies known to have carried out fraudulent practices. In fact Benford's Law is a useful tool for the IT auditor testing controls and other data sets. However, the IT auditor needs to remember to make sure that the constraints (mathematical assumptions of the theory) are compatible with the data set to be tested – Benford's Law does not hold true for all data types. Interestingly though, Benford's Law is legally admissible as evidence in the US in criminal cases at the federal, state and local levels. This fact alone substantiates the potential usefulness of using Benford's Law.

Nasty surprises

Several of my bosses over the years have run a 'no surprises' policy, and it has been something that I have adopted when I have found myself with staff reporting to me. As a manager, you want to give your staff as much free rein as possible so as not to

stifle ingenuity. However, staff with free rein will inevitably end up in sticky situations occasionally. As a manager, it is always good to find out that something horrible has happened from the offending staff member rather than from your manager. IT systems can throw up some nasty surprises, but good governance processes will take you down the path of putting in place monitoring and reporting systems that ensure that you are the first to know when the corporate website goes down; email stops working; all your products are showing up as valued at one dollar on your shop site; your security swipe card system stops working and all your staff are locked out; your automated manufacturing system has spun out of control, and so on.

One of my colleagues had an unfortunate experience when he slept through a website alert that would have warned him that the corporate website that he was supporting was no longer available. Unluckily for him, the chair of the board, who you can only suppose was suffering from insomnia and considered that a quick peek at the company website would either cure the insomnia or keep him entertained, was the first on the scene. Needless to say, a member of the company executive team was woken with a nasty surprise at an unearthly hour of the morning.



General reputation loss

All of the above can contribute to reputation loss. Good governance processes will result in 'maintaining reputation' as a business requirement at the start of any IT project, and this requirement will also be a key input to the risk register that guides the test strategy. What you mean by 'maintaining reputation' differs depending on the nature, scope and international spread of your business, services and products. In the case of a security breach, would you be more concerned about losing trust, losing money, having your intellectual property copied by competitors or losing customers? If you are a government department providing services for all citizens, your customers are a 'captive audience', so you are probably more concerned about losing trust. If you are a bank, then being perceived as a safe and secure service provider is essential, and you will recognise that your customers have a choice as to who they choose to carry out their financial services.

We had an interesting saga running in New Zealand around one of the major government payroll systems late last year. Every day we had bewildered and upset full-time and part-time staff explaining to the media that they had not been paid since the new payroll system had gone in a few months before. Having heard a number of sad scenarios, you would guess that the problems were not just a result of bad data entry and that the fundamental business rules of the system were incorrect or broken or compromised. There is never a good time to have a broken payroll system, but just coming up to Christmas must be one of the worst times.



Loss of business

Again, all of the above can contribute to loss of business, and in some cases your business could be forced to close permanently. Public memory is fairly short. If you cast your mind back to stories of some of the major corporations that experienced one of the above 'bad things' in 2011, most of them are still operating today. I think that is a tribute to the way they have reacted to the revelation that their IT systems were not as robust as they hoped. Those of us who fly a lot do not stop flying on aeroplanes after a large plane crashes killing all the passengers and the cause is suspected to be a faulty component, but we do look for reassurance before we fly again. We want to know that our chosen airline has done a thorough audit and safety check, and has 'taken on board' the 'lessons learnt' from the crash. In particular, we would like to hear proof that the root cause of the accident has been identified and addressed directly. Once we know that a faulty component has been dealt to, we might even feel safer flying than we did before the crash. However, we probably will not feel that our confidence has been fully restored until we know that the relevant airlines have adopted new processes to identify components before they fail.

Similarly, if an organisation that we deal with as a customer has a major security breach, but then carries out a thorough investigation to identify the root cause of the problem, and commissions a comprehensive independent audit and check of related systems, then that will give us confidence that at least they are taking the situation seriously. However, we are not going to be fully satisfied until we know that the organisation has adopted new governance processes and changed the way they do things to the point where the situation looks unlikely to reoccur. Whether or not the CEO or CIO falls on a sword in shame is almost immaterial. As a customer, you want to know that the organisation will operate differently in the future. And if that does not look to be the case, you will probably be taking your business elsewhere.