Turning data privacy controls projects into business benefits

In today's world, organisations face not only increasing requirements to better protect data, but also the need to utilise that data effectively and legitimately process it both internally and via support partners. Alex Ayers, Consulting Director at specialist GRC and IT security company Turnkey Consulting, describes ways of working towards the implementation of data privacy controls such that controls become benefits rather than burdens.

The US Sarbanes-Oxley ('SOx') Act of 2002 was a watershed moment for security and controls. The legislation had an unprecedented impact on organisations across the globe and, at the time, there were estimates that the total costs of achieving compliance exceeded $1 trillion. This was not long after the 'millennium bug' ('Y2K'), which had a cost of mitigation estimated at around $500 billion. The new infrastructure and applications implemented off the back of the Y2K initiatives were suddenly subject to another significant programme of work to fix problems that, outside of the accountancy firms, no one really worried about. There was a perception in the market that Enron, WorldCom et al. were due to failures in oversight so why worry about password controls and technical change management? Despite many positives coming out of SOx in the form of improved governance and controls, it is easy to see why organisations suffered from the controls fatigue that remains today.

One of the challenges that faced SOx and affects data privacy legislation is that the requirements have to be reasonably generic in order to deal with breadth of application. Regulation can be drafted in the knowledge that detail and clarification will be achieved through future legal rulings. Vendor ecosystems exist to support customers in interpreting requirements into policy. Unless failure to comply means that an organisation can no longer operate, non-discretionary projects will get the minimum funding required to achieve a minimum standard.

Public perception of the issues surrounding data privacy is at an all time high. How personal data is used and stored is changing. Organisations face competing requirements of increasing data privacy, getting insight from that data and legitimately processing it through internal teams and support partners.

Organisations often have five key questions around data privacy:

- What does data privacy mean to the business?
- What is the cost of non-compliance?
- What data has to be protected?
- How does the organisation ensure that it is compliant?
- How does the organisation make sure it remains compliant?

The answers depend on the organisation, what it does and where it operates. Larger and/or more diverse organisations can be expected to have a greater variety of answers and just determining what data privacy means to the business can be a project in itself. Organisations also take into account their appetite for risk, as the penalties for non-compliance may not be significantly punitive as to require action. With the adoption of the EU General Data Protection Regulation ('GDPR') this attitude will change as fines may run up to 2% of global revenue for an organisation guilty of the most significant breaches.

Data privacy legislation has strong parallels with SOx: they both have far-reaching implications for IT and business processes; there is no 'magic bullet'; people are the weakest link. When looking to embed data privacy controls it therefore makes sense to apply what has been learned from other controls initiatives to streamline the implementation of data privacy controls and do it in a cost effective way. We have identified four practices that can turn a data privacy controls project from a burden into a business benefit.

Change the controls mindset

Controls exist to protect value. Data privacy controls protect reputational value through avoiding privacy breaches. Controls protect financial value through the avoidance of fines, adverse publicity and ultimately the loss of current and new business. Close to every practitioner's heart, adequate controls also prevent loss of reputation and reduce the likelihood of incurring financial and operational costs through knee-jerk responses to privacy incidents.

Traditional definitions of controls such as 'preventing wrong things from happening' position controls as an overhead rather than a benefit. To engage stakeholders the value of implementing privacy controls needs to be clearly articulated and the appetite for implementation will be greatly improved.

Make it easy

If people are required to do something, it must be made easy for them. At the high level this means translating privacy requirements into policy and standards that can be implemented and audited. The policies and

standards should be delivered in a way that is meaningful for the teams who are implementing them and they should be prescriptive to allow easy auditing and to reduce the time consuming interpretation of results. At the detailed level this goes down to defining security and/or configuration settings for each relevant application or piece of IT architecture.

Activity already taking place can be leveraged and rationalised where possible. It is not unusual for different teams to be monitoring similar controls, often repeating steps at different frequencies. There can be significant commonality between compliance requirements and the related controls activities so it should be ensured that a minimum number of controls cover the maximum number of requirements. As many of those as possible should be automated to improve control effectiveness and reduce the cost of operation.

The costs of controls are usually heavily weighted towards the operational phase so investment upfront in designing efficient controls that reduce recurring cost is rarely wasted.

Integrate controls into processes

Organisations with data privacy concerns already operate controls around their key processes and should avoid creating new processes unless absolutely required. Updating existing processes and procedures as part of Business as Usual ('BaU') activity removes or reduces costs associated with doing this as part of a project. In many cases it is sufficient to top-up the knowledge of the users operating the processes through engagement and education, rather than completely re-training them. Using self-paced learning through virtual delivery mechanisms is a cost-effective way of achieving this.

Effective governance is about having the right people making the right decision with the right information

From an IT perspective, security and controls should be an integral part of every Software Delivery Lifecycle ('SDLC'). Embedding security and controls requirements in the SDLC ensures these are an integral part of the solution design. Controls are tested and test success forms part of the sign-off criteria. This gives assurance that the controls are in place and also greatly reduces the cost of implementation compared with retrofitting controls as an afterthought.

For changes to applications to meet data privacy requirements, the criticality of the change will dictate the options. Fitting changes into a scheduled release window or on the back of another project will help reduce implementation costs. A common mistake that organisations make is not to consider operating interim controls. A cost-benefit analysis should be performed against making an immediate change versus waiting for an appropriate window and using interim mitigating controls to bridge the gap. While operating the controls may come at an increased cost and have reduced effectiveness, the savings can outweigh the costs of initiating a separate project just to meet these requirements.

Operate effective governance

The previous three practices have focused on implementing controls and it is common for initiatives to finish and the effectiveness of the controls to become diluted over time. Traditional business process controls are relatively static unless processes change. Data privacy is an area that is undergoing change in a number of areas: legislation; public opinion; findings from breaches; new technology. It can be assumed that the refresh cycle for data privacy controls is more frequent than that of controls around an established business process such as purchasing.

Effective governance is about having the right people making the right decision with the right information. The key to achieving this is ensuring that everyone involved in the governance process knows their responsibilities and how success is measured. The use of authority frameworks such as RACI models is common but can still leave gaps around decision making. It can be effective to augment a governance framework with a RAPID model, which spells out decision making authority and makes it easy to align with a governance model.

Finally, policies and procedures are only any use if they result in practices. It is the practices that make or break compliance and it is the practices that are hardest to enforce. For staff and third parties to take data privacy seriously, consequences need to be in place. After ensuring staff know their roles and responsibilities, compliance with these should be included in the company assessment process and non-compliance subject to disciplinary procedures. Third parties should have obligations written into contracts and their team members working with company data should positively attest that they understand their responsibilities prior to being granted access to systems and data.

Fixing many of the data privacy challenges faced by organisations today doesn't have to be complex or expensive. Adopting some or all of the strategies above makes it straightforward to meet regulation and remain compliant, with the added benefit that they often also introduce better business practice.

Alex Ayers Consulting Director
Turnkey Consulting, UK
Contact via kate@alexandepr.co.uk