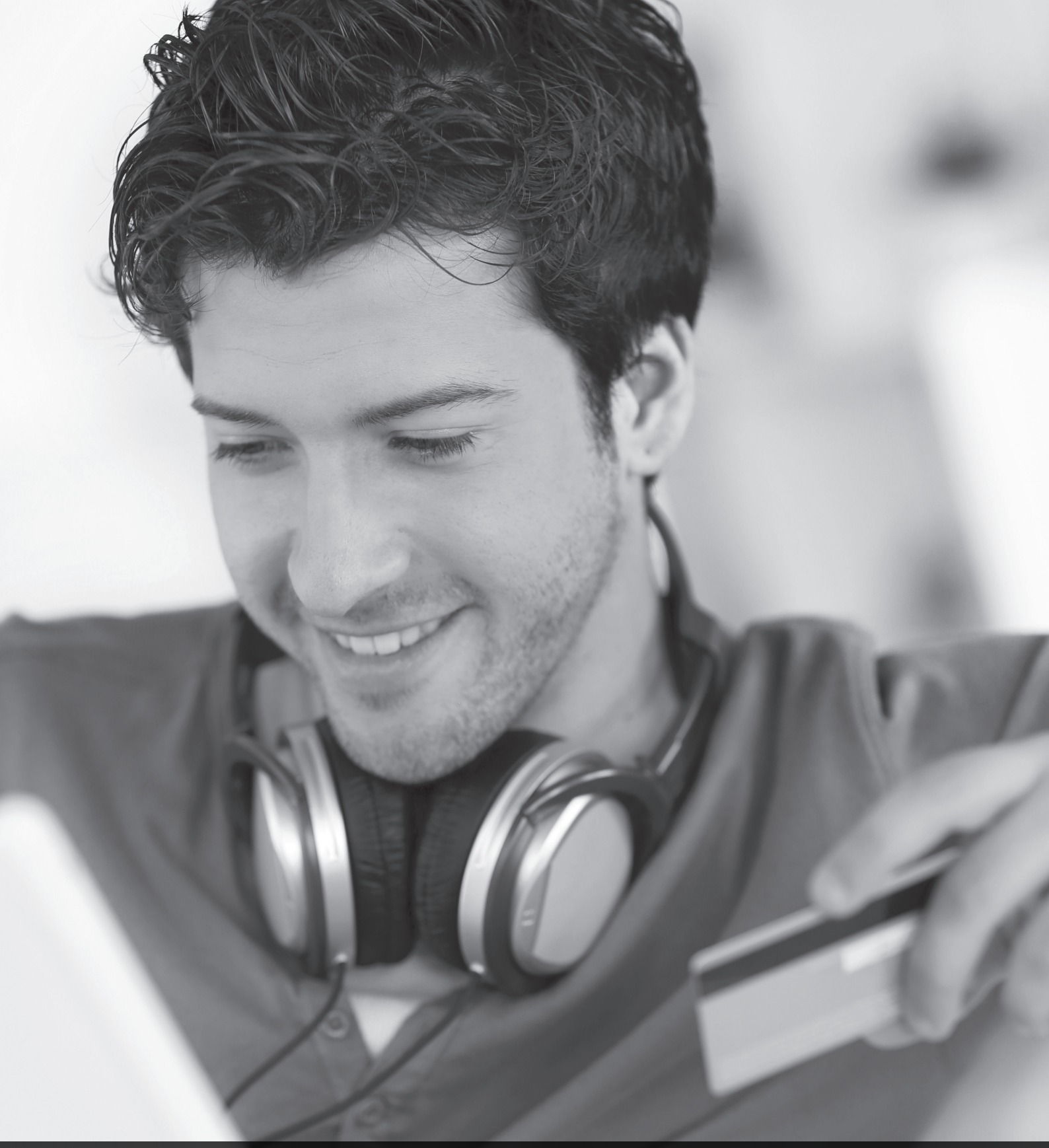


Achieving PCI DSS Compliance Through Outsourcing:

Where to begin?

August 2014

Camford

Resolving Business Challenges Through Technology

Can you achieve PCI DSS compliance through outsourcing, and if so, how should you approach it?

This whitepaper provides a brief overview of the Payment Card Industry Data Security Standard, known as PCI DSS, and details our experiences and recommendations in how to achieve PCI DSS compliance through outsourcing. For a more in-depth understanding of PCI DSS see the Further Reading section at the end of this whitepaper.

Key Terms

The world of PCI DSS is awash with acronyms. A full Glossary of Terms can be found on the PCI Security Standards website: https://www.pcisecuritystandards.org/documents/PCI_DSS_Glossary_v3.pdf.

For the purpose of this whitepaper 3 key terms are relevant:

Merchant – the organisation taking card payments from customers (i.e. your business)

Acquirer/Acquiring Bank - a bank or financial institution that processes credit and debit card payments for products or services for a merchant

Scheme – the card providers at the top of the PCI tree: Visa, MasterCard, American Express, Diners, JCB (Japan Credit Bureau)

What is PCI DSS?

All organisations processing debit and credit card transactions will be aware of PCI DSS. The global standard for cardholder account data protection, that consists of **12 core requirements**.

Under PCI DSS, every transaction that involves sensitive cardholder information must be processed, stored and transmitted securely to protect customers and businesses from the increasing threat of card fraud. However, whilst there is awareness of PCI DSS, many organisations will have business processes and IT solutions that have evolved over time and may not be compliant.

Why Should You Comply?

Compliance with PCI DSS means that systems are secure, and customers can trust you with their sensitive payment card information. Compliance improves your reputation with acquirers and payment brands, which are the partners needed in order to process card payments.

If an organisation is not compliant the consequences can be significant and may include:

- Reputational damage
- Loss of trust from customers
- Substantial Payment card issuer fines in the event of a data breach

Even without a breach having occurred, the increased risk profile will result in higher charges from the acquiring bank.

Fines

It is difficult to predict the size of a fine as information is not readily available. This is in part due to the fact that financial consequences will only be known at the time of a breach. Deloitte estimated the potential fines as follows:

"Take a quite modest compromise of 10,000 cards at a merchant, you could expect to have compromise fees of 5 euros per card; investigation costs of about 30,000 euros; an average fraud of 1,000 euros per card, card replacement costs of 20 euros per card; and 30 euros per card in chargeback fees. That comes to around 11 million euros – and 10,000 is a small example."

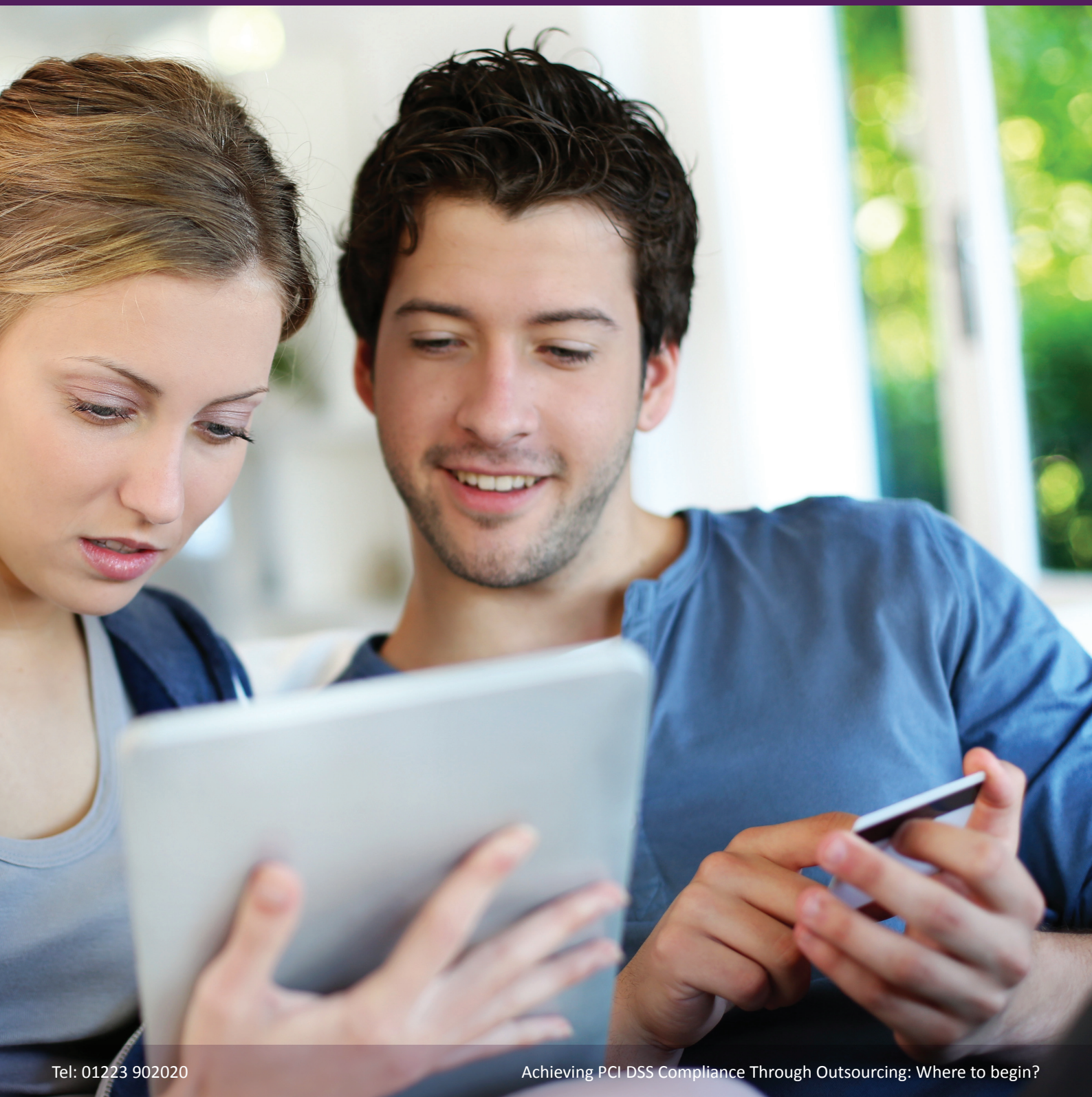
It should be noted that non-compliance does not in itself result in fines. You will only get fined in the event of a data breach, which will then be based more punitively on the number of cards put at risk, not just those that are proved compromised!

As mentioned, at the very least non-compliance will result in higher acquirer transaction fees based upon the increased risk profile. In some instances acquirers will apply additional monthly charges for not meeting compliance.

Is it easy to comply?

The level of compliance required depends on the volume of transactions and the perceived security risk of your organisation. Merchants fall into four tiers, ranging from **Tier 1** merchants who handle more than **6 million** transactions a year, to **Tier 4**, who process fewer than **20,000** e-commerce transactions per year.

Tier 1 merchants need to be audited by an independent Qualified Security Assessor (QSA), where as the others are able to self-certify. Companies that have a breach or fail to show the right attitude can be placed in Tier 1 at the discretion of the acquiring bank and regardless of their transaction volumes.



Outsourcing Considerations

There are a number of ways in which PCI DSS compliance can be outsourced. This can include full-scale business process outsourcing, such as a call centre, down to the adoption of cloud-based software solutions.

However it is essential to understand that you cannot fully outsource your compliance as the compliance responsibility remains with your organisation. Liability for PCI compliance also extends to 3rd parties involved in the business process flow. Therefore, rather than simply outsourcing the problem, you take on further responsibilities to confirm that 3rd parties are compliant. Comprehensive assessment is a vital part of understanding what elements may be vulnerable to security exploits, and where to direct remediation.

There are also many vendors who position their products and solutions as PCI compliant. These solutions do not in themselves make you and your organisation compliant. Full compliance covers the end-to-end business process in addition to the supporting technologies.

"Comprehensive assessment is a vital part of understanding what elements may be vulnerable to security exploits, and where to direct remediation."

When considering outsourcing to achieve PCI compliance the following key considerations should be taken into account:

- **The end-to-end business process** – this includes the activities of the business personnel. For example, you should avoid your customers telling your employees their Sensitive Account Data (SAD) such as card numbers, expiry dates, etc. (Sensitive Account Data – SAD). If you outsource to *'PCI compliant'* solutions, but then fail to make the business process compliant, you will have achieved little.
- **Compliance is not a one-time event** – compliance requires continual review. You cannot *'set and forget'* by outsourcing. The advantage of outsourcing is to simplify and speed up your ability to be compliant – it is not a way to enable you to transfer compliance to someone else. Also, the standard is reviewed and updated from time to time. Therefore what may be compliant now, may not be in the future. Outsourcing to a 3rd party should provide the benefit that they are on the ball and keep their solutions up to date with the standard. However there is no guarantee that they will, so you still remain responsible for keeping up to date yourself.

How to approach Outsourcing your PCI DSS Compliance

So now you know what PCI DSS is, how outsourcing can help you achieve compliance, and the key things to watch out for, how should you tackle identifying what to outsource and how to do it?

Our first recommendation is that you don't start with a vendor solution! You should start by taking a look at your organisation and identifying its current and future needs.

We have outlined below the approach we follow with our clients. It is a framework that we have had much success with and recommend that you adopt. If you have any questions on the framework, or how to apply it in your organisation, please get in touch via the details at the end of this whitepaper.

We call our process D7 and it will get you through to the implementation stage

Step 1

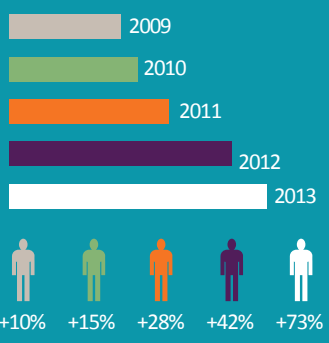
Describe existing business processes

PCI DSS is in response to the handling of credit and debit card information. The first step is to identify which processes within your business currently have this requirement. We recommend you engage with the respective business units and document each step of the process. This needn't be overly onerous if you focus at an appropriate level, limiting yourself to documenting each process within a maximum of **10** steps. In our experience we have achieved this with between **2 and 8** steps per process. Make note of where technology is used at each step. The aim is not to be too descriptive. You want to document the process so that it can be broadly understood – not to a level of a detail such that a complete novice could follow it without support.

Step 2

Discover new opportunities

Before undertaking research to determine available solutions we recommend you explore with the business any current opportunities or future business needs that would benefit from taking card payments. This can be achieved by meeting with business unit heads to seek an understanding of their business unit strategy.



Step 3

Determine the technologies in place that support the business processes

During your capture of the business processes in Step 1 you will have made a note of the supporting technologies. It is now necessary to delve into a lower level of detail to understand how technology supports each step of each business process. This includes detailing the applications and any specific IT processes, for example, overnight batch routines. The purpose of this step is to ensure you understand the IT system complexities such that any integration work can be highlighted to potential vendors.

Step 4

Document the current environment

In completing the first 3 steps you will now have a complete picture of the current business processes and their supporting technologies, along with any future potential business activities. This rich information should be collated into a single document that has two purposes:

1. It enables you to play back your understanding to the business to ensure accuracy and confirm agreement
2. This information can be included in your procurement documentation to provide vendors with an in-depth understanding of your business and IT environments in order for them to determine how their solutions may fit

Step 5

Do research to identify what vendor solutions are available

Now that you have a clear understanding of the business needs you are able to identify the most appropriate solutions and vendors. There are of course many methods of research. We recommend you consider the following:

- Engage with peer organisations in your market sector to understand what they do
- Attend conferences – there are many on the subject of PCI DSS
- Undertake internet research
- Contact vendors directly to seek literature, product demonstrations and reference sites

It is possible that during your research you identify further business opportunities. If so make note and engage with the business to seek interest/relevance. You may need to update your documentation from Step 4.

Step 6

Decide which vendor(s) solution(s) will meet your needs through a competitive procurement exercise

You now have a clear understanding of what is available in the marketplace, and you have up to date business and IT requirements. The next step is to engage your preferred vendors through a competitive procurement process.

The aims of this process are to:

- **Take advantage of the competitive market** – through a competitive procurement exercise you will get a better understanding of solution capabilities and costs
- **Ensure vendor proposals are comparable** – in running a formal procurement process, which needn't be onerous, you can compare one vendor's response from another. We recommend, however, that you allow vendors room for creativity in their responses. An RFP/ITT that is too restrictive risks missing opportunities.
- **Make certain solutions and vendors align to your organisation** – in providing the in-depth analysis of your business processes and IT environment the vendors are able to determine if you are a good fit for each other. At this early stage you are giving vendors both the opportunity to gracefully bow out, whilst enabling those that remain to start to consider solution integration, and to identify risks and challenges.

Upon completion of your analysis of vendor responses you can identify which solution(s) and vendor(s) meet your business needs. Your analysis and recommendations should be presented to the business unit leaders to agree the outcomes sought in engaging the chosen vendors, and to seek funding and approval to proceed.

You may choose to document this in a formal Business Case.

Step 7

Define a transition roadmap

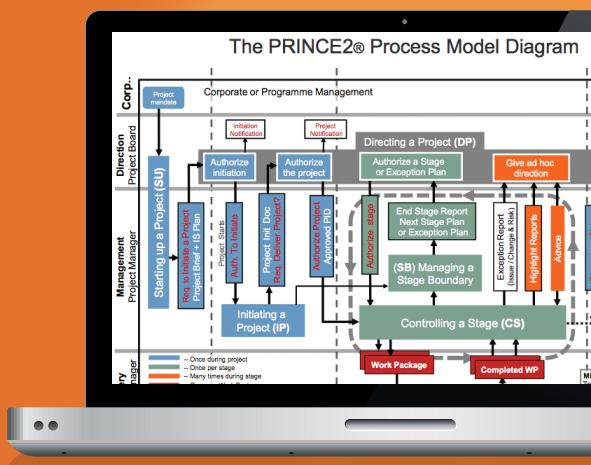
The most critical thing to remember in your transition is that this is a business project, albeit possibly led by IT. As expressed earlier, implementing any of these solutions will be futile if the business process itself does not comply with the standard.

The vendor(s) that you engage will be focused on the implementation of their technology solutions and wrap-around services. They will not be focused much, or at all, on your business process change activities or compliance. Therefore we strongly recommend that you either own the programme management, or engage an organisation independent of the vendor(s) to lead the transition and provide project/programme management on your behalf.

In defining your transition roadmap the 3 key considerations are:

1. **Engage the business** – not only will the business need to be ready to provide input to the designs and testing of the solutions, but it will also need to consider how it re-engineers business processes in order to achieve compliance and get best value from the solutions being provided
2. **Prioritisation of business processes** – target those business processes that have the highest current PCI DSS risk exposure
3. **Identify the critical path** – there may be system integration needs that require you to engage with existing 3rd party vendors. The timeframes and constraints of those vendors will need plotting in to your transition project plans. You will also want to consider any time constraints from formal notice periods with
4. existing solution providers whom you may be moving away from

At this point you will now be in a position to embark upon your implementation and transition. If you do not have an in-house project management framework we strongly recommend you adopt existing best practices and methodologies, such as **Prince2**.



Lessons Learned

In addition to the approach outlined above there are two further key lessons we have learned in supporting our clients and that we recommend you consider.

Engage expert organisations to support you

A key aspect of PCI DSS is Safe Harbour. If a merchant is the subject of a data compromise and an investigation carried out by a Qualified Security Assessor (QSA) finds the merchant to be compliant, they will benefit from what is called *"safe harbour"* and the card schemes will not fine. It is important to reiterate that in order for a merchant to be compliant, all of its third parties that would store, process or transmit cardholder data must also be compliant.

As we have repeatedly stated, PCI DSS compliance remains with your organisation regardless of the number of PCI compliant solutions you engage. You will be required by your acquirer to submit regular compliance reports and we recommend that you engage a QSA to undertake this regular review on your behalf.

The risk of potential fines, and the efforts involved in staying up to date with the PCI DSS standards, makes the engagement of a QSA a cost effective investment. Compliance shows you have taken all reasonable steps to protect the cardholder data in your charge.

Identify an appropriate owner on the business for PCI DSS

PCI DSS concerns the entire business process, not only the IT aspects. With the IT function being responsible for implementing a large proportion of the solutions, it is reasonable to assume that IT should own compliance in its entirety. We do not recommend this as the IT department does not have the relevant level of authority to command that a business unit review or change its business processes. Also, it would essentially be policing itself!

Conclusion

Even though it has been around for some years, PCI DSS can still be a daunting subject.

Whilst the standard promotes security best practice that would benefit organisations regardless, it can still be an expensive and burdensome barrier for some organisations to overcome. Utilising outsourced solutions can help you achieve compliance quicker and will likely provide further benefit as the standard evolves. Whilst you still remain responsible for compliance, we recommend you engage a QSA to further ease the pressure and to be confident that you have experts assessing your end-to-end processes.

The framework outlined above will enable you to address achieving compliance through outsourcing by putting the business processes at the centre of your considerations.

Finally, PCI DSS compliance is a business issue, not solely an IT challenge. Organisation compliance should not reside with the IT department.

Further Reading

There are a number of good sources to consult regarding PCI DSS. Here's our pick of some of the best sources:

www.pcisecuritystandards.org www.pcisecuritystandards.org/pdfs/pciscc_ten_common_myths.pdf

About the Author

Martin Williams is the Founder and Practice Leader at Camford Management Consultants.

He is a well-respected IT strategist and Programme Manager, with a clear focus on ensuring technology resolves business challenges, and that an organisation's IT function delivers value. Over a 20-year career, Martin has worked for a range of organisations, large and small, with a portfolio of clients that has taken him all across the globe. Martin can be contacted at martin.williams@camfordmc.com