FRITS J. BOS, PMP

1602 - 145 Hillcrest Ave., Mississauga, ON, L5B 3Z1 | C: (416) 524-7790 | frits@pm4hire.com

If you are accepting credit card payments directly into your application system (rather than using a payment services provider terminal) your operation ***must*** meet PCI compliance standards. While PCI Auditors evaluate compliance, they cannot recommend what is required to achieve compliance, which can result in multiple "failed" audits. Audits focus on what is wrong, not on how to fix it. That can become a very expensive way to achieve compliance one hurdle at a time.

PCI Compliance Transformation

Are you wasting money on repeated PCI compliance audits to meet PCI security standards? Keep in mind that PCI Auditors will judge: they will not advise your company on what to do to achieve compliance (that they would call a conflict of interest).

I created a custom consulting program to change that!

I offer several "service packages" I can deliver individually to address aspects of achieving PCI compliance. My focus is knowledge transfer, so your staff are prepared for an audit (if required for your operation). I am not a PCI Auditor: my experience is based on achieving the PCI PA-DSS certification for a vendor product. Based on experience, I created a 6-step process: depending on your operation you may not need all 6 steps. I perform one step at a time, so you do not incur extra costs while your staff are engaged in performing upgrades necessary to bring operations into compliance. I can advise your staff on what is required to achieve compliance and document the system for evaluation by a PCI Auditor (if a formal audit is required).

Step 1: Attestation of Compliance (1 – 5 days)

I begin by exploring (and documenting, if necessary) what card payments are processed, and how. Based on that assessment I can recommend basic preparations for an audit and prepare an Attestation of Compliance (which is addressed to your payment processor or acquirer). This "AOC" will be backed up with full documentation for the benefit of the acquirer. If it appears an actual audit is required I will help you prepare for that, based on the findings within the more limited scope of your "Attestation of Compliance" declaration.

Step 2: PCI Compliance action plan (1 – 3 days)

Based on deficiencies identified during the attestation of compliance, I do a complete review of what your acquirer and PCI will expect. This plan establishes a commitment for you to remedy any deficiencies – I can help your staff plan for the remediation steps that may be required. The attestation of compliance documentation, with a remediation action plan, may be satisfactory to your acquirer until deficiencies have been fixed, as explained below. A final review will then be performed as input to complete the attestation and file it with your acquirer service as part of their PCI compliance. Often this is all you need to do to satisfy the PCI "AOC" requirements.

If necessary, I can help you to prepare for a **PCI-DSS certification** with Step 3 and Step 4:

Step 3: Infrastructure upgrades (3 – 5 days)

If required, I can advise your IT staff on network infrastructure security improvements and/or processing infrastructure hardening and data security provisions. Sessions would be staged to give your staff time to implement improvements over a span of several months. It is important for the cardholder data to be protected from internal or external access by unauthorized people.

Step 4: Cardholder Data Protection (3 – 5 days)

Once your infrastructure meets requirements, I can help your staff to validate that there are no instances of cardholder data that can be compromised. I also advise on data encryption at rest, as well as in communications (which is usually dictated by the acquirer service). You may need to implement physical access restrictions to the card processing area and establish procedures to protect physical media which (of necessity) may contain cardholder data (such as order forms).

If you develop software things can get a bit complicated!

When you replace acquirer-provided equipment with custom software solutions, you may need "**PA-DSS**" standards compliance. A vendor-provided system may already be certified, but, if you customize that software, you enter a gray area that might require both the vendor and your version of the software to comply with "**PA-DSS**" standards, which will require a full PCI Audit.

Step 5: Secure Software Development (5 – 10 days)

One of the aspects the PCI Auditor looks at is your standards and guidelines for secure software in your organization. Don't sweat the small stuff – I have documentation for that and all I need to do is put your corporate identity on the documents. I can hold training sessions for your development staff so that (1) they are familiar with the contents, and (2) you have fulfilled that training requirement with a signed attendance sheet. I can advise your development staff to isolate card processing components that contain unredacted cardholder data, to minimize the overall footprint of payment card processing within your software applications domain. I can also help you to develop technical documentation to emphasize the PCI-relevant components.

Step 6: PA-DSS Audit Preparation (1 - 3 days)

The final step before engaging the PCI auditor for a "Report On Vendor" is for us to complete the checklist of items that the auditor will most likely look for, and to provide a guide that helps you to answer the most likely question scenarios, as well as to establish the scope of the software.

Low cost introductory offer

For this ***introductory offer*** we charge $850.00 per day (for out-of-town venues add $400.00 for travel time, plus reimbursement of transportation and lodging expenses at cost).

Respectfully,

Frits J. Bos, PMP