# Ahmed Almass, Kieth Wu, & Ong Mehm

# Module 8: PCI Domains and Requirements

## Case Study Part C

After many meetings and discussions, it’s time to start implementing PCI controls based on the report you received from the QSA. There are many aspects to the project, including network configuration, data protection, vulnerability management, access control, monitoring and policies. It can be overwhelming but with planning and the support of your leaders, it can be done.

* Your QSA will work with you to develop the implementation plan based on their findings.
* Support from your IS team and the Finance department will be required to make changes to network and system configurations.
* The Finance department will also help to modify the business processes for staff members that handle credit cards.
* You will need to engage Employee Services to help implement training for all staff that handle credit cards, including any new employees.
* Your executive team will provide guidance and approval for policy creation and communication to staff.

As you can see, it’s a team effort, not just another IT project.

Implementation of the PCI domains and requirements is difficult and time-consuming, but you won’t be finished until you achieve compliance by finding an Approved Scanning Vendor (ASV) and have four consecutive, successful vulnerability scans with no errors. You will then have to complete a Self-Assessment Questionnaire (SAQ) and an Attestation of Compliance (AOC), and submit this paperwork to your payment processor for review. They may ask for further clarification or evidence before providing you with your report of compliance. From this point, you must keep the controls up-to-date and operating effectively, in addition to regular scanning so that you can keep compliant year over year.

In groups of four, answer the following questions using the PCI Gap Analysis document from student resources area of BrightSpace.

1. How many decisions regarding both mandatory and optional implementation items are in the report?

There are 12 decisions that are required before the 13 mandatory and 7 optional.

1. Can the IT department do this without involving any other departments?

Though possible, it would not be recommended. A holistic scope is required for a successful and healthy implementation that factors in the experiences and needs of all parties this policy will affect, which should be most if not all employees in the organization.

1. Where do you start?

We would recommend to start with seeking the guidance of a QSA, prepare what levels of decisions are best for your network. Then move onto the 13 mandatory and 7 optional decisions. Then get your network checked if its PCI DSS compliant.