Industry
Media and Entertainment

Client’s Profile
The customer is an integrated company providing e-commerce as well as information and communication services. Offering online services in several fields such as employment, continuing education, housing, automobiles, personal, social networks and classification ads; it attracts almost 8 million unique visitors per month in Canada.

The Challenge
The customer was facing several regulatory requirements involving important changes in its internal processes and technology. One of these requirements was from the Payment Card Industry (PCI). From an information security perspective, it was unclear the implications of such requirements as well as the required efforts to move forward to a compliance process.

The Payment Card Industry (PCI) Data Security Standard (DSS) is a set of specific security requirements for companies that process, transmit or store payment card information. This comprehensive standard is intended to help organizations protect customer account data and reflects most of the usual best practices for securing sensitive information.

The Solution
Since the customer had no clear understanding about PCI requirements implications, and given that its compliance project was in its initial stage, our approach for this mandate was to perform a comprehensive Gap Analysis in relation to PCI DSS requirements:

- We started by performing a business processes analysis in order to identify payment options as well as cardholder information to be protected.
- We evaluated the customer’s security controls currently in place, in comparison to specific requirements established in the PCI DSS. During this evaluation, we considered human, technical and administrative aspects.
- We performed a comprehensive revision of all information security documentation available.
- Our network design team was also involved in the technical review of critical IT infrastructure elements, in particular, network architecture.
- As a result from this process, we produced a detailed report showing all gaps between security controls in place and PCI DSS requirements.
- Finally, we provided the customer with a list of recommendations and a proposed action plan in order to correct identified gaps.
Case Study: Compliance to PCI

The Benefits

This project allowed our customer to:

- Understand the PCI DSS requirements implications;
- Identify missing security controls in relation to PCI DSS requirements;
- Develop administrative and procedural security controls as required by the PCI DSS;
- Identify cost-effective security measures that will help to reduce PCI scope and compliance costs;
- Design a detailed implementation plan to achieve PCI DSS compliance;
- Improve overall organization’s security posture;
- Benefit from PCI DSS security controls implementation to achieve compliance to others regulatory requirements.

Services provided by Above Security on the occasion of this project

We supported our customer through our PCI services portfolio including pre-audit and gap analysis services. In addition, our consulting team provided proper recommendations about secure network architecture oriented to facilitate PCI DSS compliance.

Above Security has experience into the field of compliance for many international standards, in particular: World Lottery Association, Basel II, HIPAA, PCI, etc.

About Above Security

Our mission is to be our customers’ strategic partner in information risk management. Above Security helps more than 250 organizations throughout 22 countries in the Americas, Caribbean, Europe and North Africa. Our clientele is composed of organizations in almost all sectors namely: finance, banking, insurance, pharmaceutical, telecommunications, manufacturing and government entities.

Since 1999, Above Security allows you the peace of mind you deserve to achieve your business objectives.