

Data Protection Assessment



Solution Overview

Technological advances have fostered growth and efficiency in the payments industry while simultaneously creating opportunities for a wide variety of criminal and fraudulent activities to flourish. In an effort to stem illegal activity and protect sensitive cardholder data, card associations, regulatory agencies, as well as state and federal legislatures, have mandated various initiatives, such as Sarbanes-Oxley, data protection legislation and Visa's Cardholder Information Security Program, that require organizations to implement security controls and programs to protect such information. Perhaps the most damaging threat is the havoc created within a firm's customer base when customer information – addresses, PINs, passwords, or account numbers – are compromised. This not only threatens the integrity of the client base and the payments infrastructure in general, it also exposes a firm to litigation, penalties and business interruption losses.

Business Needs

In many businesses today, fraud has become an unwanted cost of doing business. As new relationship opportunities and payment options present themselves, devious individuals and organised criminals find lapses and voids in safeguards and create financial losses. Perpetrators are continuously devising schemes and techniques targeted at financial institutions, card issuers, acquirers, processors, retailers and Internet businesses. JCO Group's Data Protection Assessment is designed to be a flexible yet thorough approach to identify and benchmark fraud prevention processes and systems. Emphasis is on process improvement and consideration of industry best practices.

Business Solutions

A Data Protection Assessment begins by aligning business, operations, and system objectives with industry mandates and legislative requirements. A thorough assessment and situation analysis of current policies, practices and methods of fraud prevention and data protection is performed. A comprehensive gap analysis of industry best practices and requirements is undertaken and suggested improvements are determined. Projects will often focus on a number of functional areas, making sure that there is alignment between overall business objectives and business processes. Once completed, you will be prepared for any required audits.

Areas of expertise include banking, retail, online commerce, payment processing and business relationship management that requires strong identity verification. Typical engagements focus on the effective use of available data, identifying best of breed solutions combined with an effective management approach and process improvement.

Practically all businesses that are prone to security and data compromise find that an effective program of ongoing analysis and continuous process improvement provides the greatest level of efficacy and financial loss prevention with the lowest impact on business operations, customer relationships and revenue

Company Information

JCO Group provides planning, analysis, definitional, advisory and marketing services to leading organizations in the payments industry that seek to improve their performance, efficiency and profitability through the use of best practices and technology. JCO Group has assisted many clients around world implement practical, cost effective solutions to address the challenges and opportunities that clients face.

**Data Protection Assessment
A Proven Path Process**

PROJECT PHASE	DURATION	PROJECT DELIVERABLES
Step One: Assessment	3-16 weeks elapsed time	Determine current state, gap analysis, project plan for required development and implementation, recommend policies and safeguards, present to stakeholders
Step Two: Development and Implementation	4-12 weeks elapsed time	Using project plan, modify and/or create and implement policies, structures, system remediation plans to secure and protect vital data that are capable of complying with association and regulatory security audits
Step Three: Review / Ongoing Support	2-3 weeks elapsed time	Support for association audit (and ongoing periodic audits), if required, changes in security requirements, modify services and systems, may require reviews in order to upgrade / update security measures in order to maintain compliance.