



# RKON Virtual CSO Whitepaper

---

Demystifying PCI-DSS Compliance  
for Your Organization

**Version 1.0: Feb 11, 2011**

**Authored by: Chris Serafin, *RKON Senior Security Architect***

# CONTENTS

- How RKON’s Virtual CSO can Demystify PCI-DSS Compliance in your Organization ..... 1
- VCISO Summary ..... 3
- RKON VCISO - Best Practice Strategy..... 3
  - Architecting and Supporting a Secure Environment..... 3
  - Protecting Cardholder Data ..... 3
  - Mature Vulnerability Management – Maintain and Secure ..... 4
  - Proactive Log Monitoring and Alerting of the Cardholder Environment..... 4
  - Implementing Strong Access Controls ..... 4
  - Maintain your Policies like Living Entities..... 4
  - Separation of Duties ..... 4
  - Economies of Scale ..... 5

## VCSO Summary

---

It's no secret that many organizations fear the acronym PCI-DSS. Some think PCI is an unattainable goal, others think PCI does not adequately protect the business against today's mutating and blended threats, and others don't realize that if you handle cardholder data, you are obligated to comply. Regardless of your stance is on PCI-DSS, RKON's Virtual CSO can help you bridge the gap so you are in a position to safely gauge your organization's risk posture.

While most organizations have a dedicated workforce handling IT operations, the *overall security vision* often gets tossed aside due to day-to-day responsibilities, internal project work, putting out fires, and limited resources. This can be a challenge for small and medium businesses (SMBs) that must comply with PCI or other forms of regulatory compliance and a CSO/CIO is absent from the corporate structure.

Many SMBs require a visionary leader who can step up and own responsibility for increasingly complex governance, risk, and compliance projects. Virtual CSO is that visionary leader—an industry expert who can be entrusted to handle your demanding security vision and risk model, enabling your staff to focus on internal projects and day-to-day operations.

## RKON VCSO - Best Practice Strategy

---

To RKON, PCI-DSS is nothing more than a security best practice that organizations should have always been following. We understand that this may be easy for the large enterprise that allocates capital resources towards it, but more of a challenge for an SMB with limited resources. RKON has devised a VCSO or best practice strategy to assist SMBs with this challenge, which includes: Architecting and supporting a secure environment; Protecting cardholder data; Mature vulnerability management; Proactive Log Monitoring and Alerting of the Cardholder Environment; Implementing Strong Access Controls; Maintaining Policies; and Separation of Duties.

### Architecting and Supporting a Secure Environment

Most organizations know that you need to implement at least a firewall as a first line of defense for your network. But what happens when organizations have a high number of policy changes? Continual firewall modifications tend to create rule redundancy and/or rule subversion, which can expose the organization to allowing more access than required to complete legitimate business activity. For this reason, our firewall audits uncover that SMB firewalls may have a more secure firewall rule set than a *Fortune* 500 enterprise. Regardless of what your accepted change control may authorize, engineering mistakes happen—both by accident or inexperienced engineering—and hopefully not on purpose. Regularly scheduled vulnerability assessments, outsourced firewall management, and perimeter security audits verify that the agreed upon security measures are in place and maintained as outlined by your risk management policies.

### Protecting Cardholder Data

The tenet of the PCI-DSS requirement is the *Principle of Least Privilege*, meaning you only get access to what you need to complete a business transaction: nothing more, nothing less. Access is data stored (if it's allowed), both physically and during transit, even over insecure mediums such as the Internet. The name of the game here is: if you don't need it, get rid of it. Storing of cardholder data should be as short as possible to limit liability, and should be purged quarterly. Let's face it: the three-spoke firewall model is dead. No longer are we dealing with WAN, LAN, and DMZ separation. Today's basic networks have at least dual WAN zones, multiple LAN segments, and should be implementing a plethora of DMZ levels to segregate tiered security zones to properly segment and minimize a security breach. Together with properly segregated DMZs, disk encryption, and adhering to the Principle of Least Privilege RKON's VCSO offering can successfully help you protect cardholder data.

## Mature Vulnerability Management – Maintain and Secure

The majority of IT management understands the importance of a successful vulnerability management practice. Few manages, however, align this best practice with the significant ROI that can result—and not only in terms of compliance. From malware mitigation, disabling default credentials and insecure protocols, to implementing a patching cycle and pro-active web application penetration testing: a mature vulnerability management practice speaks volumes to your risk posture strategy. With regular vulnerability assessments and securing any issues found, VCSO helps you main and secure your systems and vital applications. RKON’s VCSO team combines a number of commercial and open-source tools along with specialized web application testing partnerships to provide clients with enterprise-level vulnerability management and a full SDLC for their applications.

## Proactive Log Monitoring and Alerting of the Cardholder Environment

Network and application monitoring is the lifeline for reacting to anomalies and outages in your environment. While most enterprise clients have a Syslog/SNMP solution in place, real-time monitoring and alerting to an overabundance syslog, SNMP traps, Netflow, and a number of router, firewall, and HIDS/NIDS logging can easily overwhelm a client infrastructure. Taking all of these multiple silos of data and importing them into a central repository is called Security Event and Incident Management (SEIM). SEIM solutions have been notorious for being non-intuitive and costly for years. For the SMB and even large enterprise, getting your foot in the door is around \$100K and requires a full time engineer to maintain without providing great return of value for the organization. Outsourcing this portion of SEIM to a qualified third party, like RKON VCSO, can help you maintain compliance, provide complete 24x7x365 coverage of alerting, and provide compelling return on investment.

## Implementing Strong Access Controls

Microsoft’s Active Directory is everywhere, and for the most part it does a good job as a directory service. The enterprise struggle is by not having a strong vision of what a properly tiered security approach should look like from the very beginning. While this tiered approach is pretty much default in most directory services, many companies see employees as a domain admin or a basic user. Having a well-defined security hierarchy combined with dual-factor authentication, allows organizations to practice the ‘Principle of Least Privilege’ and provide for non-repudiation in the cardholder environment.

## Maintain your Policies like Living Entities

When RKON asks if the client has any security policies to audit, the answer is usually *no* or *yeah somewhere*. The latter is usually in a dusty binder underneath a stack of old Cisco 2500s—neither followed nor updated to reflect the current environment. Your network is a fluid, dynamic entity and your security policies should be as well. Properly updated documentation and policies should be as mandatory as changing default credentials. If there is one thing that stuck with me from a college professor, it was “You live and die by documentation.” All polices should be updated as needed and audited quarterly for proper change control and a basic sanity check. Most enterprise clients lack the resources to adequately maintain the policies, so this is another opportunity for Virtual CSO can help bridge the gap.

## Separation of Duties

Separation of power is the key tenet of governance, risk, and compliance; yet, this separation can be a major hurdle for many enterprise clients. The primary goal of separation of duties is to prevent fraud, errors, and keep auditors smiling. Having a governance body outsourced to a trusted third party, like RKON, can help to provide valuable insight into industry trends and best practices. Outsourcing allows you to gain the collective experience from thousands of client environments, not just your own.

**Economies of Scale**

To successfully run a security practice, organizations need four-five very different skills sets but often only have the budget for one. Companies may hire a great firewall engineer but he often lacks audit and policy skills or visa versa. RKON's VCISO service allows you to buy a small portion of five different, highly trained experts so you get the experience of a world class security team for a fraction of the cost—often for less than you can hire one person for.

**About RKON**

At RKON, we care about providing our clients with world-class IT services, support, and long-term relationships. We strive to provide superior client satisfaction while offering services to architect, implement, and support technology solutions that are secure, scalable, and highly available—on site or in the cloud. Learn more at [RKON.com](https://www.rkon.com) or contact RKON at: [solutions@rkon.com](mailto:solutions@rkon.com) | t: 312.654.0300.