Feature

Incorporating COBIT Best Practices in PCI DSS V2.0 for Effective Compliance

Mathew Nicho, Ph.D., CEH, SAP-SA, RWSP, is an assistant professor of information systems at the College of Information Technology of the University of Dubai (UAE). He also conducts a professional course on ethical hacking for IT professionals. Nicho can be contacted at *mnicho@ud.ac.ae.*

Payment Card Industry Data Security Standard version 2.0 (PCI DSS v2.0) was released by the PCI Security Council in October 2010 and comes with clarifications and guidance that expand upon the previous version. With more and more transactions based on credit cards, merchants dealing with these are forced to comply with standards such as PCI DSS v2.0 or face huge penalties. As PCI DSS v2.0 is generic in nature while highly specific with in-depth, focused controls, merchants are finding it costly and increasingly difficult to implement and interpret this standard. COBIT, initially released in 1995 with the latest version released in 2007 (and an update scheduled for release in early 2012), has much in common with PCI DSS and comes with detailed methodology and guidance. A comparison of the two frameworks reveals that the effectiveness of PCI DSS can be enhanced by using the best practices of COBIT.

In 2008, US customers spent US $2.5 trillion in transactions via credit cards at 24 million locations in 200 countries and territories.[1] With 10,000 payment transactions made every second worldwide,[2] there is good reason to ensure that cardholder information is kept secure. By the end of 2009, there were 576.4 million credit cards and 507 million debit cards in circulation in the US alone, which equates to roughly 3.4 cards for every person in the US.[3] Since most transactions are done electronically using cardholder information, there is an ever-increasing need to ensure the protection of cardholder data. The security of cardholder data has become a more serious concern to businesses worldwide. The reasons for this include high-profile and persistent data breaches,[4] regulatory concerns in financial services and other industries, enactment of regulations regarding reporting of data breaches, changes to court rules requiring availability and proof of integrity of electronically stored information submitted as evidence, and tangible and intangible losses due to breaches.[5] As such, ensuring effective and efficient implementation of PCI DSS v2.0 goes a long way toward securing transactions and mitigating breaches. Viewed from a wider information systems (IS) perspective, the most critical issue facing IT executives is not securing cardholder data, but rather aligning (IT) goals with business goals. IT executives are under pressure to be more flexible, to manage constant change from internal and external sources, to align IT services with business requirements, and to implement business practices.

Experts have argued that PCI DSS should be integrated into the wider IT governance (ITG) domain, since ITG is made up of five core pillars—security, compliance, cost, enablement and efficiency—which are vital for a holistic implementation of IS security.[6] By focusing on these five areas, rather than on just compliance and security, IT managers can move away from an "in place—not in place" approach to PCI DSS v2.0 compliance to one of wider security governance. Since every IT control standard, tool and framework has its own strength and limitation, it makes sense to incorporate the best practices of an appropriate framework into PCI DSS v2.0. IT security, thus, cannot be confined to the PCI DSS focus of securing cardholder data alone, but needs to diverge to the wider IT security perspective to include IT control and assurance. While PCI DSS v2.0 is prescriptive, when a control cannot be implemented for business reasons, there is ample opportunity to replace the specific requirements of the standard with compensating controls, providing equal or greater protection.[7] Research on standard setting has found that incorporating the various interests of the IS network into the governance structure, along with flexibility to satisfy competitive interests, is the key to success.[8]

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

Go directly to the article:

PCI DSS

Introduced in 2005, PCI DSS is the very first and perhaps the only industrywide standard that focuses mainly on protecting cardholder data. The PCI Security Council is an open, global forum founded by the five global payment brands: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. The council was created for developing, managing, educating and communicating the PCI Security Standards, including PCI DSS, the Payment Application Data Security Standard (PA-DSS), and the Personal Identification Number (PIN) Transaction Security (PTS) requirements to merchants, vendors and financial institutions involved in credit card transactions. The objective of the council is to enhance the security of cardholder data and, thus, to help facilitate global adoption of consistent data security measures created to mitigate data breaches and prevent payment cardholder data fraud. Compliance is enforced, by the PCI Security Standards Council, on those dealing with credit cards, and there are penalties for nonconformance to PCI DSS.

ISSUES WITH COMPLIANCE

A study of 500 US and multinational organizations found that, on average, it was necessary to dedicate 35 percent of an organization's security budget to any compliance effort.[9] In a 2009 survey, the UK Corporate IT Forum (CIF) estimated that only 1 percent of the surveyed companies were fully PCI-compliant, that 9 percent failed their audit and that the rest were trying to achieve compliance.[10] Thus, merchants dealing with credit cards are faced with two cost extremes. First, enterprises face the risk of credit card transaction breaches and fraud along with penalties for not complying with the PCI standards. Second, they face huge costs in complying with the PCI standards. For example, in 2008, level-one merchants (those dealing with more than 6 million transactions per year) spent an average of US $3.38 million to become PCI-compliant, including the cost of PCI assessment services.[11] Since 2006, merchants have collectively spent in excess of US $1 billion on compliance to PCI DSS.[12] Becoming PCI-complaint does not mean that the company is insulated from all cyberfraud, but effective implementation can mitigate the risk to a great extent. While PCI DSS v2.0 promises better protection than the former version, there is still room for improvement.

> "Becoming PCI-complaint does not mean that the company is insulated from all cyberfraud, but effective implementation can mitigate the risk to a great extent."

Security Breaches—Lack of an Effective Compliance Mechanism

Even with increasing compliance to standards and regulations, there has been no decrease in attacks on networks. Symantec recorded more than three billion malware attacks in 2010.[13] If recent and former cases are analyzed, it is evident that attacks are becoming more nontechnical and targeted (targeted attacks target employees to penetrate an organization and stay hidden) in nature. A few significant cases follow:

- Starting with a sophisticated attack, one of the most sensational technical data breaches occurred at TJX Companies Inc. in 2006. That year, the enterprise ranked 133rd on the Fortune 500 list. With revenues reaching US $17 billion, 125,000 employees and more than 2,400 stores worldwide, TJX was classified as the largest off-price apparel and home fashions retailer in both the US and the world. However, in late 2006, hackers broke into the systems of TJX and stole vital customer information with estimated losses (tangible and intangible) amounting to US $1 billion—one of the largest security breaches ever reported.[14]
- A less technical breach occurred in 2008 at Hannaford, a PCI-compliant supermarket chain. The data breach, which resulted in reported thefts of 4.2 million customer credit and debit card numbers with 1,800 cases of fraud, began on 7 December 2007. Unusual credit card activity became known on 27 February 2008; the breach was not contained until 10 March 2008 or reported until 17 March 2008. It was later found that unauthorized software that was secretly installed on servers in most of the company's supermarkets enabled the massive data breach.[15, 16, 17]

- Moving toward a nontechnical attack, in 2010, two sensational cases of targeted attacks (spear-phishing) occurred—Stuxnet and Hydraq. The Stuxnet malware, which infected Iranian nuclear plant networks, was reported to have been inserted into the network through a Universal Serial Bus (USB) device. Rather than sabotage, the intention of the Hydraq malware was to steal intellectual property from companies through unsuspecting employees who downloaded the e-mail attachment that contained the hidden malware.
- The 2011 data breach of RSA, an enterprise that provides security, risk and compliance solutions, was disclosed on 17 March 2011 to the US Securities and Exchange Commission. In this case, the attackers used spear-phishing, in which e-mails were sent to two small groups of lower-level employees with the e-mail subject "2011 Recruitment Plan." The e-mail went to the junk mail folder, but one employee retrieved it from the junk mail folder and opened the Excel file attachment. The spreadsheet contained a zero-day exploit that installed a backdoor through an Adobe Flash vulnerability.[18, 19]

These breaches show that focusing on protecting cardholder data alone will not provide adequate security. **Figure 1** shows a comparative study of how breaches occurred for the years 2007 to 2010 based on statistical studies conducted by Verizon during these years.[20] As shown in **figure 1**, nontechnical and human factors are still regarded as a formidable threat, which the PCI DSS standard alone cannot prevent. Insertion of malware, physical theft, privilege misuse, social engineering and errors mostly fall under the nontechnical umbrella of hacking.

Figure 1—Methodology of Breaches

	2007	2008	2009	2010
Hacking	59%	64%	40%	50%
Malware	31%	38%	40%	49%
Physical theft	15%	9%	15%	29%
Privilege misuse	*	22%	48%	17%
Social engineering	*	*	28%	11%
Significant errors	62%	67%	*	*

*No studies on this type of attack are available for this year.

Source: Verizon, *2011 Data Breach Investigations Report*, USA, 2011

Compliance with PCI DSS considerably reduces risk and liability for the company, but it is not a guarantee for full protection against data breaches. According to the 2010 Verizon study on the payment card industry, organizations that suffered a data breach were 50 percent less likely to be compliant than the normal population of PCI clients.[21] However, it is not easy to become PCI-complaint. Of the merchant companies assessed by VeriSign Global Security Consulting Services, 79 percent were cited for noncompliance in their PCI audit due to failure to protect stored data.[22] Thus, it is vital for information security management programs to not only extend to other IS domains, but also to view IS security from a holistic ITG perspective rather than from an IT perspective.

ITG VIEW OF IS SECURITY

Viewing IS security from an ITG perspective, information security management is defined as the process of administering people, policies and programs, with the objective of assuring continuity of operations while maintaining strategic alignment with the organizational mission.[23] This strategic alignment requires PCI DSS v2.0 implementation not only to diverge from its focused domain and expand to its outer concentric rings of the greater IS domain, it also forces PCI DSS v2.0 to link to the organizational strategic goals, which is a major concern for IS managers. In surveys published by the IT Governance Institute (ITGI) in 2006 and 2008, the importance of strategic alignment of organizational goals with IT goals was cited as vital to the organization by 90 percent of the respondents.[24, 25] Hence, irrespective of the dynamic nature of the IS domain over the years, the issue of aligning the PCI DSS/IT goal of securing cardholder data with the higher-level organizational goals remains a concern even today. Therefore, an isolated solo approach to PCI DSS v2.0 implementation may not be effective in creating a secure IS environment for holding cardholder information.

Evaluating IT Controls

While PCI DSS has been grouped under information security standards,[26] COBIT, as a framework, incorporates perspectives of information security. COBIT is internationally recognized, accepted and widely used as a high-level governance and control framework with processes and control objectives that focus on information security. It is comprehensive and based on 41 international source

documents, providing a global perspective and a best practice point of view.[27] COBIT divides IT activities into four domains:
1. Plan and Organize (PO)
2. Acquire and Implement (AI)
3. Deliver and Support (DS)
4. Monitor and Evaluate (ME)

These domains comprise 34 processes and 222 control objectives. Incorporating one framework into another framework involves evaluation and comparison of the two. Like pieces of a jigsaw puzzle, each of the components of PCI DSS and COBIT have been analyzed, compared and contrasted to find common ground to converge on a strategic fit.

Integrating PCI DSS With COBIT

While COBIT is viewed as comprehensive and generic, PCI DSS guidelines/requirements have much depth, are specific and go into the finer details of compliance. PCI DSS v2.0 comes with six principles and 12 requirements. Each of these 12 requirements is further subdivided into lower-level requirements (with corresponding testing procedures). Experts have termed the 12 requirements as "core," "basic" and "high-level," and the lower-level requirements (with corresponding testing procedures) as "subrequirements."[28, 29, 30] As the PCI DSS v2.0 requirements follow a multilevel numbering format (e.g., 1, 1.1 and 1.1.1), for the purpose of differentiating them in this article, the 12 requirements are referred to as "core," and the lower-level requirements (with corresponding testing procedures) are referred to as "level-two" and "level-three" subrequirements. Thus, there are 45 level-two subrequirements and 75 level-three subrequirements (with corresponding testing procedures for each). In a similar manner, COBIT consists of four processes (corresponding to the six principles of PCI DSS v2.0) and 222 control objectives (corresponding to the 12 core requirements of PCI DSS v2.0). From a detailed analysis of the 222 control objectives, it can be seen that these can be segmented further to correspond to the 45 level-two subrequirements and 75 level-three subrequirements of PCI DSS v2.0. COBIT further elaborates the control objectives with "control practices" that can be equated with the "testing procedures" of PCI DSS v2.0. From the perspective of COBIT, the missing links in PCI DSS are seven information criteria (effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability); the Responsible, Accountable, Consulted and Informed (RACI) charts; IT goals; and metrics.

Structurally, the COBIT controls and PCI DSS v2.0 have much in common. While COBIT encompasses IS entirely into four domains, 34 processes, 222 control objectives, corresponding IS control practices, and related goals and metrics, PCI DSS, when viewed from the perspective of COBIT, focuses on only a few COBIT controls (out of the 34 processes), such as DS5 *Ensure systems security.* Here, the difference between DS5 and the PCI DSS v2.0 is that the COBIT controls are broad and generic rather than specific, as in PCI DSS v2.0. Viewed from the perspective of PCI DSS, the standard corresponds to COBIT with its six principles, 12 core requirements, 120 level-two and level-three subrequirements (with corresponding testing procedures), and compliance checklist for the testing procedures.

As PCI DSS v2.0 is focused on a specific domain of IS, it covers only a small percentage of the COBIT framework; however, the standard can be incorporated either as a separate domain or within the controls. As COBIT offers flexible options for customizing its processes to suit different organizations, auditors take different approaches when implementing the framework. The rationale for using COBIT as an information security governance framework is that it integrates information security into the controls of the whole ITG framework.

While implementing COBIT, it is common to start at the high-level control processes and then define the activities, but it is not uncommon to take a more granular approach by starting at the high-level control processes, defining the corresponding detailed control objectives, defining detailed corresponding activities, and then arriving at the IT goals and metrics. At the same time, responsibility and accountability for the activities/task are addressed through the use of the RACI chart, which states that the enterprise and IT function personnel who are to be held responsible or accountable are to be informed or consulted for undertaking the activities. Finally, the activities are linked to the goals and are measured using quantitative measures that show the activities' current state in relation to the IT goal, using measures such as "degree of approval," "degree of compliance," "percent of," "level of satisfaction" and "delay between." The seven information criteria, RACI chart and specific measures provide a much more effective, efficient and focused overview of the different IS entities.

Integration of COBIT best practices within PCI DSS v2.0 entails analyzing the implementation process of both to evaluate the similarities and differences, so as to identify the areas where relevant COBIT best practices can be incorporated into PCI DSS v2.0. With this objective, a COBIT control process related to information security and a corresponding PCI DSS v2.0 requirement are used to illustrate the respective implementation process flow (**figures 2** and **3**).

Figure 2—COBIT Process DS5

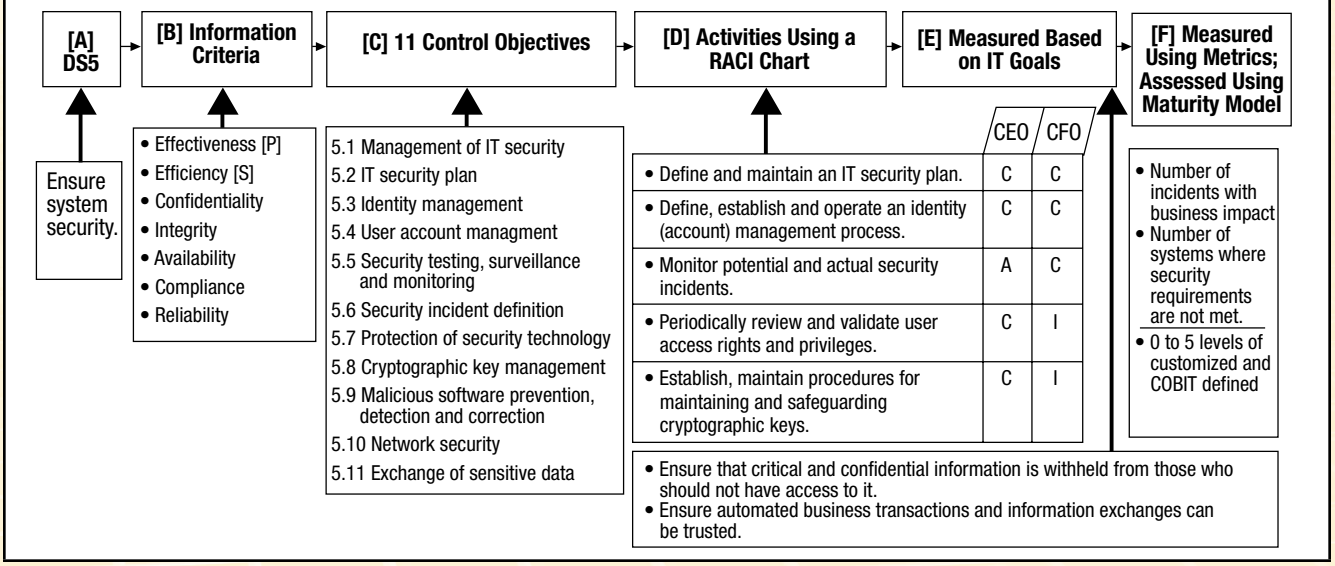
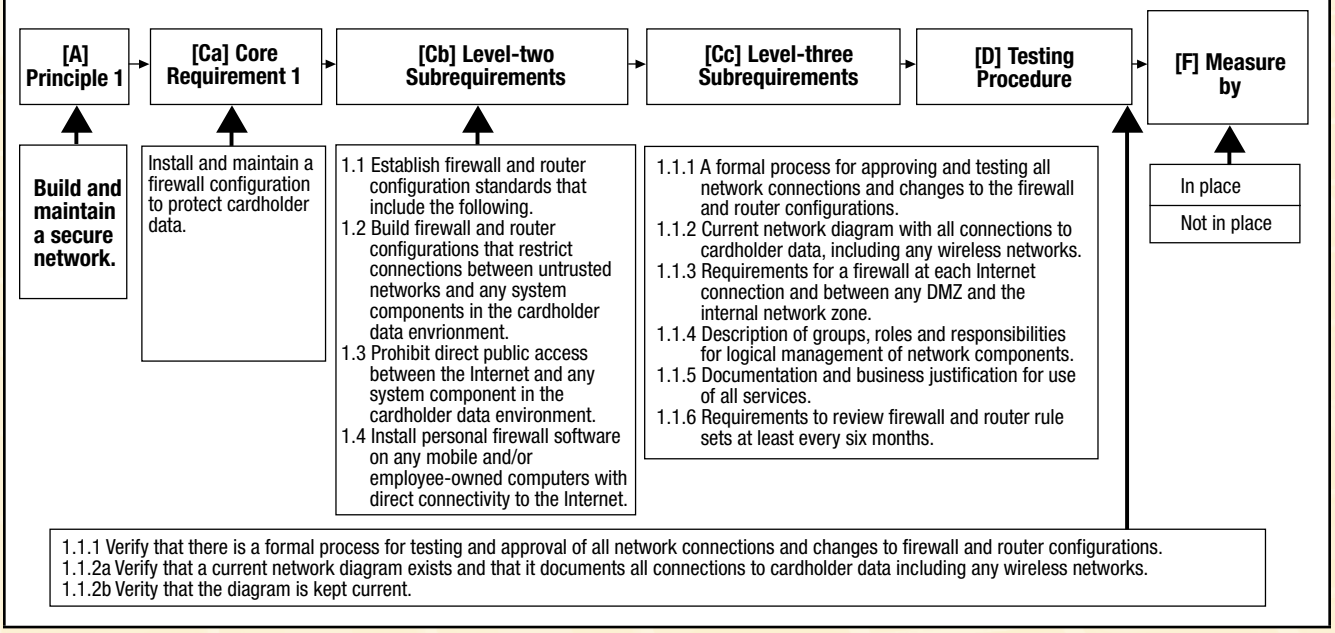


Figure 3—PCI DSS Core Requirement 1 of Principle 1



In the example, the COBIT high-level control process DS5 is evaluated using two of the seven information criteria. COBIT defines these criteria to evaluate a control process to characterize the controls and assign priority, whether any one or more of these criteria are primary or secondary to the selected control process. Since PCI DSS v2.0 does not include these criteria (see [B] in **figure 2**), a similar set of criteria has been defined in the expanded confidentiality, integrity, availability (CIA) triangle of the US National Security Telecommunications and Information Systems Security Committee (NSTISSC) model of information security, which focuses on IS security, namely confidentiality, integrity, availability, possession, utility, accuracy and authenticity.[31] This expanded CIA triangle can be applied to the six principles, 12 core requirements or the 45 level-two subrequirements of PCI DSS v2.0, which provide an IT security focus rather than an IT governance focus.

In **figure 2**, DS5 is further broken down into 11 control objectives and segregated into activities that correspond to the COBIT control objectives. Similarly, in **figure 3**, PCI DSS v2.0 principle one [A] is broken down into one requirement [Ca], and four level-two subrequirements [Cb], and six level-three subrequirements [Cc] (with corresponding testing procedure 1.1.1, 1.1.2a and 1.1.2b for level-three subrequirements 1.1.1 and 1.1.2 [D]). Here, PCI DSS v2.0 goes deeper technically than COBIT, but it is missing the RACI chart that equates to the level-two and/or level-three subrequirements and/or testing procedures.

> "PCI DSS v2.0, with just a unidimensional measurement visibility, lacks the measurement depth of COBIT."

As PCI DSS v2.0 is highly specific and detailed, incorporating the four components of the RACI chart ensures greater assurance and control with the standard. The RACI chart identifies the participants; to what degree they interact with defined activities; how they make decisions; and the positions, roles, activities, and decision areas or functions. The RACI matrix is a valuable tool for reducing the conflict between IT and business.[32]

Considering the measurement perspective ([F] in **figure 2**), COBIT uses compliance (similar to PCI DSS v2.0 "in place/not in place"), measures and metrics (such as number, rating scale, percentage and average), and the COBIT maturity model. In addition, consultants who implement COBIT also use red, amber and green color-coding to denote "noncompliant," "may be complaint" and "fully compliant," respectively. This multi-measurement approach not only provides greater visibility, it also aids in tracking the progress of a control over time. Moreover, the maturity level aids in assessing the level of the standard in relation to the industry. PCI DSS v2.0, with just a unidimensional measurement visibility, lacks the measurement depth of COBIT.

Proposed Model

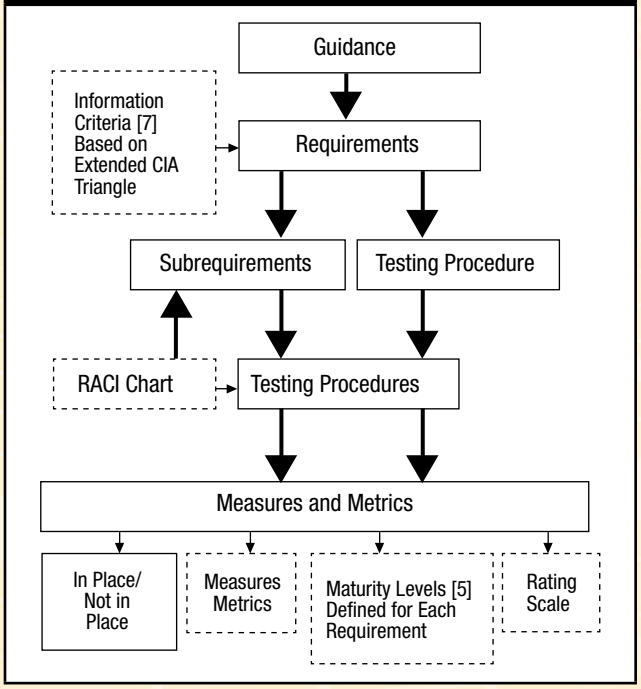
The most successful programs view PCI DSS v2.0 as a holistic cycle that needs to be continuously monitored and maintained.[33] Taking into account a holistic perspective of PCI DSS v2.0 and the gaps located in PCI DSS, the best practices of COBIT that can be incorporated into PCI DSS are:

- The expanded CIA triangle (based on the COBIT information criteria format) to provide prioritized context to the selected principles and/or requirements, which will not only provide more focus to the principle/requirement, it will also identify the criteria with which each of the PCI DSS requirements is assessed
- The RACI chart to specify roles and responsibilities, which will not only make IT personnel accountable and responsible for a particular principle/requirement, it will also provide guidance to the personnel on who is to be informed and/or consulted for each requirement
- A multidimensional measurement framework to provide a full view of the principle/process; to undertake regular trend analysis through tracking the performance of each of the principles, core requirements, and level-two and -three subrequirements over a period of time through the use of appropriate metrics and corresponding/rating scales; and to assess the maturity level of the entire PCI DSS in that company that is relative with the industry. The resulting model of PCI DSS v2.0 incorporating the relevant best practices of COBIT is given in **figure 4**.

While the expanded CIA triangle and the RACI chart can be incorporated into PCI DSS v2.0 without much effort or many amendments, incorporating a multidimensional measurement framework faces three hurdles. First, the main issue in developing the measurement framework is identifying a metrics generation model to define a set of metrics for the

core requirements, level-two subrequirements and/or level-three subrequirements because these metrics need to be aligned with the principles and the core requirements. Second, a PCI DSS v2.0 maturity model (MM) needs to be developed along the lines of the COBIT MM (**figure 5**) for each requirement (defining each of the five maturity levels in one, two or three sentences for each of the 12 core requirements). Third, for generating trend analysis reports on the level of compliance, appropriate rating scales need to be defined for

Figure 4—Extended PCI DSS V2.0



the core requirements, level-two subrequirements and level-three subrequirements or metrics that are recorded at regular intervals and tracked over time. Moreover, the huge number of lower-level quantified measures that are generated from the principles and the requirements need to be statistically aggregated and summarized to provide dashboards for different managerial levels.

CONCLUSION

Being PCI-compliant may not be enough to keep an organization's IS secure; hence, there is a need for enterprises that deal with cardholder information to integrate PCI DSS v2.0 with appropriate frameworks to fill the gaps in the

Figure 5—COBIT MM

1—Processes are *ad hoc* and disorganized.
2—Processes follow a regular pattern.
3—Processes are documented and communicated.
4—Processes are monitored and measured.
5—Good practices are followed and automated.

standard. It has been argued by practitioners and researchers alike that IT security research has failed to produce practical solutions to growing security threats.[34] Therefore, the extended PCI DSS v2.0 model proposed at a conceptual level in this article needs to be empirically tested and evaluated in different industry sectors and geographic locations to validate and generalize the model. The conceptual model can be automated into a user-friendly program using a front-end application and a back-end populated (PCI DSS v2.0) database. This model can be given to organizations for independent evaluation and the responses can be recorded, analyzed and incorporated into the current model to come up with a commercial solution for benefiting the wider business community.

ENDNOTES

1 Woolsey, Ben; Matt Schulz; "Credit Card Statistics, Industry Facts, Debt Statistics," *CreditCards.com*, 14 July 2011, *www.creditcards.com/credit-card-news/credit-card-industry-facts-personal-debt-statistics-1276.php*

2 *Ibid*.

3 *Ibid*.

4 Liebowitz, Matt; "2011 Set to Be Worst Year Ever for Security Breaches," *SecurityNewsDaily*, 9 June 2011, *www.securitynewsdaily.com/2011-worst-year-ever-security-breaches-0857*

5 Goodman, Seymour; Rob R. Ramery; "Global Sourcing of IT Services and Information Security: Prudence Before Playing," *Communications of the Association for Information Systems*, vol. 50, issue 20, 2007

6 Coburn, Alan; "Fitting PCI DSS Within a Wider Governance Framework," *Computer Fraud & Security*, September 2010

7 Owen, Michael; Colin Dixon; "A New Baseline for Cardholder Security," *Network Security*, June 2007

[8] Sullivan, Richard J.; "The Changing Nature of US Card Payment Fraud: Issues for Industry and Public Policy," paper presented at the Workshop on the Economics of Information Security Harvard University, 21 May 2010

[9] Everett, C.; "PCI DSS: Lack of Direction or Lack of Commitment?," *Computer Fraud & Security*, December 2009

[10] *Ibid*.

[11] Amato-McCoy, D. M.; "The Next Phase of PCI Security," *Chain Store Age*, July 2009

[12] First Data, *PCI DSS and Handling Sensitive Cardholder Data—Why You Care*, USA, 2009

[13] Symantec, Symantec Internet Security Threat Report vol. 16, 2010, *www.symantec.com/business/threatreport/*

[14] Xu, William; Gerald Grant; Hai Nguyen; Xianyi Dai; "Security Breach: The Case of TJX Companies, Inc.," *Communications of the Association for Information Systems*, vol. 23, 2008

[15] Wilson, Tim; "Hannaford, Security Industry Hunt for Cause of Massive Breach," Security Dark Reading, 18 March 2008, *www.darkreading.com/security/application-security/211201282/hannaford-security-industry-hunt-for-cause-of-massive-breach.html*

[16] Harkavy, Jerry; "Secret Software Blamed for Hannaford Breach," MSNBC.com, 28 March 2008, *www.msnbc.msn.com/id/23846014/ns/technology_and_science-security*

[17] ConsumerAffairs.com, "Hannaford Bros. Faces Class Action Over Data Breach," 21 March 2008, *www.consumeraffairs.com/news04/2008/03/hannaford_data2.html*

[18] US Department of Homeland Security (DHS), Vulnerability Summary for CVE-2011-0609, National Vulnerability Database, USA, 22 September 2011, *http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0609*

[19] Rivner, Uri; "Anatomy of an Attack," Speaking of Security, RSA, 1 April 2011, *http://blogs.rsa.com/rivner/anatomy-of-an-attack/*

[20] Verizon, *2011 Data Breach Investigations Report*, USA, 2011

[21] Verizon, *Verizon 2010 Payment Card Industry Compliance Report*, USA, 2011

[22] *Op cit*, First Data

[23] Choobineh, Joobin; Gurpreet Dhillon; Michael R. Grimaila; Jackie Rees; "Management of Information Security: Challenges and Research Directions," *Communications of the Association for Information Systems*, vol. 20, 2007

[24] IT Governance Institute (ITGI), *IT Governance Global Status Report—2006*, USA, 2006

[25] ITGI, *IT Governance Global Status Report—2008*, USA, 2008

[26] Tsohou, Aggeliki; Spyros Kokolakis; Costas Lambrinoudakis; Stefanos Gritzalis; "A Security Standards' Framework to Facilitate Best Practices' Awareness and Conformity," *Information Management & Computer Security*, vol. 18, issue 5, 2010

[27] Lainhart, John W. IV; "COBIT: An IT Assurance Framework for the Future," *The Ohio CPA Journal*, January-March 2001

[28] Kadambi, S. Kiran; Jun, Li; Alan H. Karp; "Near-field Communication-based Secure Mobile Payment Service," paper presented at the 11th International Conference on Electronic Commerce, Taiwan, 2009

[29] Moeller, Robert; *IT Audit Control and Security*, Wiley, USA, 2010

[30] Ataya, George; "PCI DSS Audit and Compliance," *Information Security Technical Report 15*, 138–144, 2010

[31] Whitman, Michael E.; Herbert J. Mattord; *Principles of Information Security, 3rd Edition*, Course Technology Inc. USA, 2009

[32] Wende, Kristin; "A Model for Data Governance—Organising Accountabilities for Data Quality Management," paper presented at the 18th Australasian Conference on Information Systems, Australia, 2007

[33] Coburn, Alan; "Fitting PCI DSS Within a Wider Governance Framework," *Computer Fraud & Security*, September 2010

[34] Julisch, Klaus; "Security Compliance: The Next Frontier in Security Research," paper presented at New Security Paradigms Workshop, 2008, USA