Comparison of PCI DSS and ISO/IEC 27001 Standards

Tolga Mataracioglu, CISA, CISM, COBIT Foundation, CCNA, CEH, ISO 27001 LA, BS 25999 LA, MCP, MCTS, VCP, is chief researcher at TUBITAK BILGEM Cyber Security Institute in Turkey. He is the author of many papers about information security published nationally and internationally. His areas of specialization are system design and security, operating systems security, information security management systems, business continuity, COBIT®, and social engineering.

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card companies, including Visa, MasterCard, American Express, Discover and JCB. PCI DSS "was created to increase controls around cardholder data to reduce credit card fraud via its exposure."[1] "[The] ISO/IEC 27001 standard is a specification for an information security management system (ISMS) published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) under the joint ISO and IEC subcommittee."[2]

While both standards focus on information security, ISO/IEC 27001 is suitable for every type of organization and PCI DSS focuses on organizations dealing with e-commerce.

What if those two standards were to be combined? Is that feasible? What are the differences between the standards?

This article discusses and examines the interoperability of PCI DSS 3.1 and ISO/IEC 27001:2013. Further, the pros and cons of the PCI DSS and ISO/IEC 27001 standards are compared and contrasted.

PCI DSS

PCI DSS is a standard developed by a council consisting of Visa, MasterCard, American Express, Discover and JCB in order to preserve payment card and cardholders' sensitive information.[3] There are six goals and 12 requirements in the standard (**figure 1**).

These 12 requirements have been addressed at a high level in ISO/IEC 27001:2013 standard

Figure 1—Overview: 12 Requirements of PCI DSS

PCI Data Security Standard: High-level Overview	
Build and maintain a secure network and systems.	1. Install and maintain a firewall configuration to protect cardholder data.
	2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect cardholder data.	3. Protect stored cardholder data.
	4. Encrypt transmission of cardholder data across open, public networks.
Maintain a vulnerability management program.	5. Protect all systems against malware and regularly update antivirus software or programs.
	6. Develop and maintain secure systems and applications.
Implement strong control access measures.	7. Restrict access to cardholder data by business need to know.
	8. Identify and authenticate access to system components.
	9. Restrict physical access to cardholder data.
Regularly monitor and test networks.	10. Track and monitor all access to network resources and cardholder data.
	11. Regularly test security systems and processes.
Maintain an information security policy.	12. Maintain a policy that addresses information security for all personnel.

Source: Tolga Mataracioglu. Reprinted with permission. Based on PCI Security Standards Council, *PCI DSS Quick Reference Guide,* October 2010, *https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf*

Figure 2—High-level Mapping of PCI DSS Requirements to ISO/IEC 27001	
PCI DSS Requirement	**ISO/IEC 27001 Clause**
1. Install and maintain a firewall configuration to protect cardholder data.	A.12 Operations security A.13 Communications security
2. Do not use vendor-supplied defaults for system passwords and other security parameters.	A.12 Operations security A.13 Communications security
3. Protect stored cardholder data.	A.12 Operations security A.13 Communications security
4. Encrypt transmission of cardholder data across open, public networks.	A.14 System acquisition, development and maintenance
5. Protect all systems against malware and regularly update antivirus software or programs.	A.14 System acquisition, development and maintenance
6. Develop and maintain secure systems and applications.	A.14 System acquisition, development and maintenance
7. Restrict access to cardholder data by business need to know.	A.12 Operations security A.13 Communications security
8. Identify and authenticate access to system components.	A.12 Operations security A.13 Communications security
9. Restrict physical access to cardholder data.	A.11 Physical and environmental security
10. Track and monitor all access to network resources and cardholder data.	A.12 Operations security A.13 Communications security
11. Regularly test security systems and processes.	A.14 System acquisition, development and maintenance A. 6 Organization of information security A.18 Compliance
12. Maintain a policy that addresses information security for all personnel.	A.5 Information security policies
Source: Tolga Mataracioglu. Reprinted with permission.	

developed by the ISO and the IEC. **Figure 2** shows high-level mapping of these 12 PCI DSS requirements to ISO/IEC 27001:2013 clauses.

Companies must be audited by a qualified security assessor (QSA) and an approved scanning vendor (ASV) in predetermined periods that have been authorized by the PCI Council.[4] Further, the Internal Security Assessor (ISA) can perform assessments using self-assessment questionnaires (SAQs), depending on the size and the level of the merchants.

Figure 3 illustrates the compliance of PCI DSS in four different levels based on number and type of transactions. **Figure 4** depicts the compliance of JCB. **Figure 5** portrays the compliance of American Express. These three figures help organizations by providing information on how to audit information security within the context of the number of transactions performed annually. By using the information in the following figures, chief information security officers (CISOs) can easily decide in what circumstances to perform a self-assessment, a security scan or an on-site review for auditing information security.

Figure 3—Compliance of PCI DSS		
Merchant Level	**Merchant Definition**	**Compliance**
Level 1	More than 6 million V/MC transactions annually across all channels, including e-commerce	Annual onsite PCI data security assessment and quarterly network scans
Level 2	1,000,000-5,999,999 V/MC transactions annually	Annual self-assessment and quarterly network scans
Level 3	20,000-1,000,000 V/MC e-commerce transactions annually	Annual self-assessment and quarterly network scans
Level 4	Less than 20,000 V/MC e-commerce transactions annually and all merchants across channel up to 1,000,000 VISA transactions annually	Annual self-assessment and annual network scans
Source: Tolga Mataracioglu. Reprinted with permission. Based on Compliance Resource Kit, What Is PCI DSS, *complianceresourcekit.com/index.php?option=com_content&task=view&id=67*		

Figure 4—Compliance of JCB

If cardholder data and transaction data are handled via the Internet or Internet-accessible network:

	Merchants		Payment Processors
	One million JCB transactions or more per year	Less than 1 million JCB transactions per year	Regardless of the number of JCB transactions
Self-assessment	N/A	✓	N/A
Security scan	Quarterly	Quarterly	Quarterly
Onsite review	Yearly	N/A	Yearly

If cardholder data and transaction data are not handled via the Internet or Internet-accessible network

	Merchants		Payment Processors
	One million JCB transactions or more per year	Less than 1 million JCB transactions per year	Regardless of the number of JCB transactions
Self-assessment	N/A	✓	N/A
Security scan	N/A	N/A	N/A
Onsite review	Yearly	N/A	Yearly

Source: Tolga Mataracioglu. Reprinted with permission. Based on JCB, JCB Data Security Program, *partner.jcbcard.com/security/jcbprogram/index.html*

Figure 5—Compliance of American Express

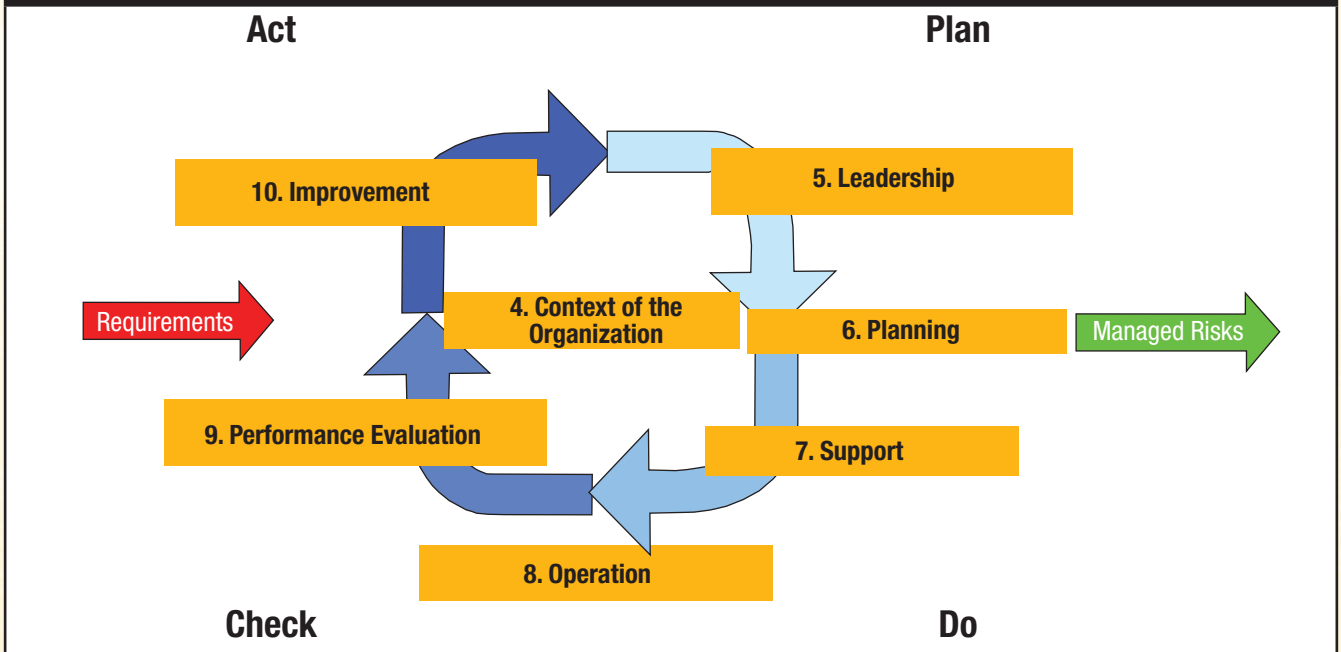
Levels	Explanation
Level 1	2.5 million or more American Express card transactions per year
Level 2	50,000 to 2.5 million American Express card transactions per year (Service providers: fewer than 2.5 million transactions)
Level 3 designated	Fewer than 50,000 American Express card transactions per year and have been designated by American Express as being required to submit validation documents
Level 3	Fewer than 50,000 American Express card transactions per year (merchants only)
Level EMV	50,000 or more American Express chip-enabled card transactions per year with at least 75 percent made on an EMV-enabled (chip-enabled) terminal capable of processing contact and contactless American Express transactions

Source: Tolga Mataracioglu. Reprinted with permission. Based on American Express, The Data Security Operating Policy, *https://www209.americanexpress.com/merchant/services/en_US/data-security*

ISO/IEC 27001 STANDARD

This standard includes seven main titles within the scope of annex SL: organization, leadership, planning, support, operation, performance evaluation and improvement.[5] Annex SL is a new management system format that helps streamline creation of new standards and make implementing multiple standards within one organization easier. It was created by ISO Technical Management Board's (TMB) Joint Technical Coordination Group (JTCG).[6] Using the same titles defined in the annex SL is useful for those organizations that choose to operate a single management system that meets the requirements of two or more management system standards. Although ISO/IEC 27001 does not suggest a Plan-Do-Check-Act (PDCA) cycle, the seven titles can be mapped into the cycle as shown in **figure 6**.

Figure 6—Mapping of ISO/IEC 27001 Titles Into PDCA Cycle



Source: Tolga Mataracioglu. Reprinted with permission.

ISO/IEC 27001 contains 14 control domains, shown in **figure 7**, and 114 controls.

Figure 7—The 14 Control Domains of ISO/IEC 27001

Control Domains	Number of Controls
A.5: Information security policies	2
A.6: Organization of information security	7
A.7: Human resources security	6
A.8: Asset management	10
A.9: Access control	14
A.10: Cryptography	2
A.11: Physical and environmental security	15
A.12: Operations security	14
A.13: Communications security	7
A.14: System acquisition, development and maintenance	13
A.15: Supplier relationships	5
A.16: Information security incident management	7
A.17: Information security aspects of business continuity management	4
A.18: Compliance	8
TOTAL:	114

Source: Tolga Mataracioglu. Reprinted with permission. Based on International Organization for Standardization, ISO/IEC 27002, Information technology—Security techniques—Code of practice for information security controls, *www.iso.org/iso/catalogue_detail?csnumber=54533*

COMPARISON OF THE STANDARDS

InformationShield has developed a table that provides high-level mapping between the security requirements of PCI DSS and ISO/IEC 27001.[7]

It is recommended that combining both PCI DSS and ISO/IEC 27001 provides better solutions about information security to organizations. The flexibility of ISO/IEC 27001 is higher than that of PCI DSS, since all of the controls have been written at a high level.

"The organizations have to determine the boundaries and applicability of the information security management system to establish its scope."[8] When comparing the scope of the two standards, scope selection in ISO/IEC 27001 depends on the company; however, the scope is exactly the credit cardholder information in PCI DSS.

Although the controls in ISO/IEC 27001 are recommendations, it is important to note that the controls in PCI DSS are compulsory.

Since ISO/IEC 27001 is more flexible than PCI DSS, it is easier to conform to the ISO/IEC 27001 standard.

When comparing the costs, establishing a typical information security management system (ISMS) and completing the PDCA cycle costs approximately US $150,000 in a typical organization. The cost of a typical PDCA cycle includes:[9]

- The costs that are caused by information security incidents
- The costs for managing information security
- The costs that are related to information security measures
- The costs of capital that are induced by information security risk

However, the cost of compliance with PCI DSS is approximately US $120,000 to US $700,000, due to the differences among the four levels.

And what about auditing? Recertification auditing of ISO/IEC 27001 is performed in three-year cycles and small-scope auditing is performed every year. There are also surveillance audits that are performed at least once a year. In contrast, there are four network scanning audits and an onsite audit for level 1 in PCI DSS.

There are compliance levels in PCI DSS to measure the maturity level of the company; no compliance levels exist in ISO/IEC 27001.

Mapping of PCI DSS and ISO/IEC 27001 is shown in **figure 8**.

Figure 8—Mapping of PCI DSS and ISO/IEC 27001:2013

Parameter	ISO/IEC 27001:2013 Standard	PCI DSS
Creator	ISO	PCI Council
Flexibility	High	Low
Scope	Depends on the company	Credit cardholders' information
Controls applied	Flexible	Tight
Controls	High-level	Low-level
Control types	"Should"	"Must"
Compliance	Easy	Hard
Number of controls	114	224
Auditing	Three-year cycles and a small-scope audit performed every year	Four network scanning audits and an onsite audit for level 1
Certification	May be given to all companies	Any companies that provide information security for critical paying processes
Compliance level	Does not exist	Exists

Source: Tolga Mataracioglu. Reprinted with permission.

CONCLUSION

PCI DSS is a standard to cover information security of credit cardholders' information, whereas ISO/IEC 27001 is a specification for an information security management system. Mapping of PCI DSS and ISO/IEC 27001 standards is vital information for managers who are tasked with conforming to either standard in their organizations. It is recommended that PCI DSS and ISO/IEC 27001 be combined to give better solutions about information security to organizations.

ENDNOTES

1 CDS, PCI Security Standards Council, *cdsus.com/default/PCICompliance.php?url=PCICompliance&PHPSESSID=bdd07f210c2e5109832eee383d0b1656*

2 International Organization for Standardization, Technical Commitees, *www.iso.org/iso/home/standards_development/list_of_iso_technical_committees.htm*

3 PCI Security Standards Council, What Is the PCI Security Standards Council?, *www.pcisecuritystandards.org/security_standards/role_of_pci_council.php*

4 PCI Security Standards Council, *Payment Card Industry Data Security Standard Approved Scanning Vendors*, May 2013, *https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v2.pdf*

5 Tangen, S.; A. Warris; "Management Makeover - New Format for Future ISO Management System Standards," International Organization for Standardization, 18 July 2012, *www.iso.org/iso/news.htm?refid=Ref1621*

6 The 9000 Store, ISO 9001:2015 in Detail: What is the New Annex SL Platform?, *the9000store.com/iso-9001-2015-annex-sl.aspx*

7 InformationShield, PCI-DSS Policy Mapping Table, *www.informationshield.com/papers/ISO27002%20PCI-DSS%20V3%20Policy%20Map.pdf*

8 International Organization for Standardization, ISO/IEC 27001 Information Technology—Security Techniques—Information Security Management Systems—Requirements, *www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103*

9 Brecht, M.; T. Nowey; *A Closer Look at Information Security Costs*, working paper, The Workshop on the Economics of Information Security, *www.econinfosec.org/archive/weis2012/papers/Brecht_WEIS2012.pdf*