International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Comparative Study between PCI-DSS v4.0 and ISO/IEC 27001:2022

Adesh Mukati[1], Dr. Astitwa Bhargava[2]

Email: *adeshmukati.1998[at]gmail.com*
https://orcid.org/0000-0001-6449-2508

Email: *astitwa.nliu[at]gmail.com*

Abstract: ***This research article presents a comparative study of the Payment Card Industry Data Security Standard (PCI-DSS v4.0) & the International Organization for Standardization's (ISO) 27001: 2022 standard, focusing on their approaches to information security management. The study analyses the key differences & similarities between the standards, focusing on their approaches to information security management. PCI-DSS v4.0 primarily focuses on securing payment card data, while ISO 27001: 2022 provides a broader framework for managing information security risks for all types of information assets. The study evaluates the benefits & challenges of implementing both standards, highlighting the need for significant resources & careful planning. The integration of both standards can align an "organization's information security efforts with global best practices & ensure continuous" improvement. The study recommends that organizations carefully assess their information security needs & resources before deciding to implement both standards.***

Keywords: Payment Card Industry Data Security Standard (PCI-DSS v4.0), International Organization for Standardization (ISO) 27001: 2022, Payment card data, Information security management system, Financial information

1. Introduction

The year 2022 is anticipated to be an intriguing period for information governance, particularly in the realm of compliance frameworks. The initial phase of the year saw the release of the latest edition of the international standard for information security management systems, ISO 27001: 2022, & soon after, version 4.0 of the PCI-DSS standard is unveiled. The publication of the ISO 27002: 2022 guidelines has demonstrated significant improvements & updates to the "**Annex A**" controls. However, it's worth noting that even with all these changes, there are fundamental aspects of information governance that have not been altered.

The ISO 27001: 2022 is released during the fourth quarter of 2021, with the corresponding guidance on implementation outlined in ISO 27002: 2022 being made available in February 2022. Organizations are allotted approximately 18 to 24 months to make the transition to the new standard.

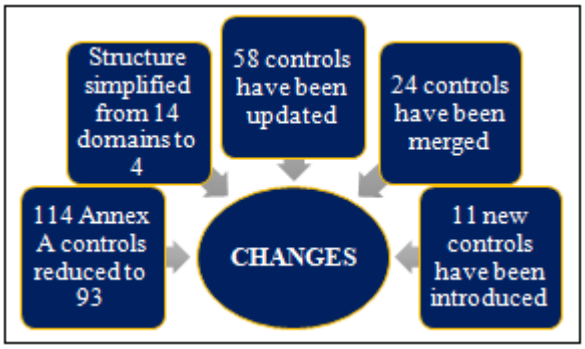

Figure 1: Changes in ISO 27002: 2022

On March 31, 2022, the PCI Security Standards Council (PCI-SSC) published an updated version of its standard, which grew from 139 pages to 360 pages. The updated standard includes elucidations, definitions, flowcharts, & illustrations that elucidate how to interpret & implement it. This indicates that the PCI-SSC recognizes that previous iterations of the standard were excessively vague for organizations to comprehend, resulting in numerous instances of noncompliance.

Licensed Under Creative Commons Attribution CC BY

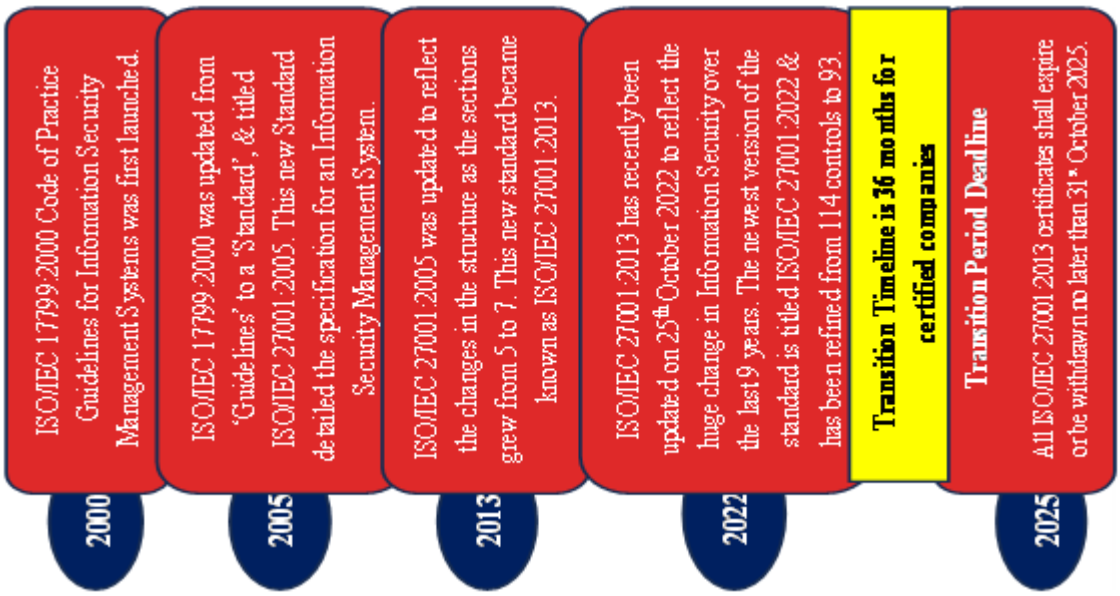

Figure 2: ISO 27001: 2013 has been updated to ISO/IEC 27001: 2022

Similar to ISO 27001, organizations are granted 24 months to migrate to the latest PCI-DSS standard. Furthermore, akin to ISO 27001, the modifications introduced in the new standard are incremental, rather than transformative. As an illustration, a single term has been modified out of the six clauses (or groups) comprising PCI-DSS.

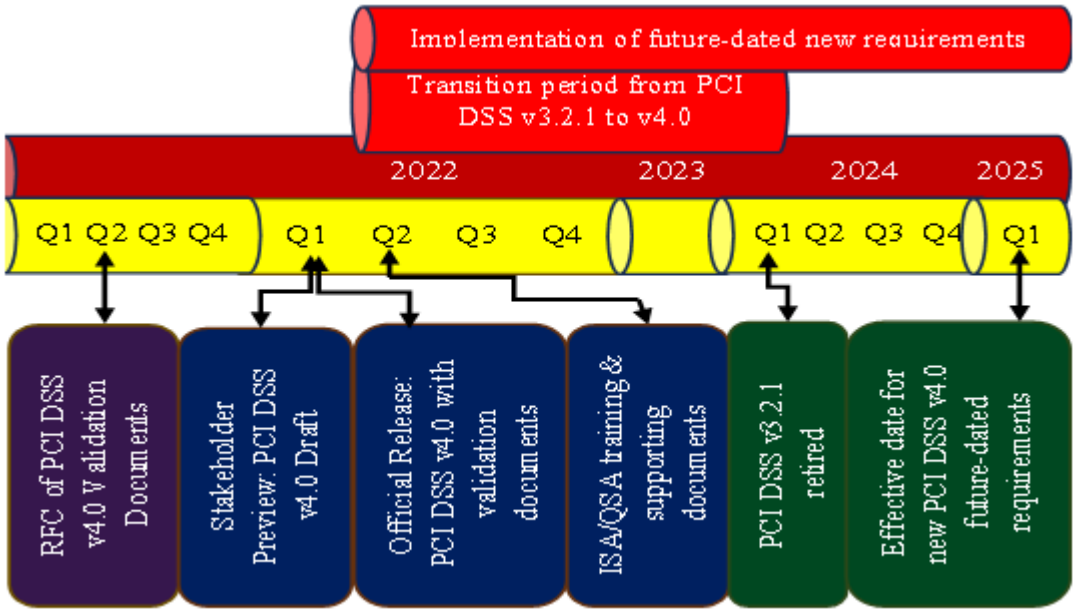

Figure 3: PCI-DSS v4.0 Transition Timeline

Table 1: Changes to clauses in PCI-DSS v3.2.1 & v4.0 0

PCI-DSS v3.2.1	PCI-DSSv4.0
Build & Maintain a Secure Network & Systems.	Build & Maintain a Secure Network & Systems.
Protect **Cardholder** Data.	Protect **Account** Data.
Maintain a Vulnerability Management Program.	Maintain a Vulnerability Management Program.
Implement Strong Access Control Measures.	Implement Strong Access Control Measures.
Regularly Monitor & Test Networks.	Regularly Monitor & Test Networks.
Maintain an Information Security Policy.	Maintain an Information Security Policy.

While it may appear to be a minor alteration, the new standard has made an effort to replace references to "cardholder data" with "account data" wherever feasible. Although the terms had been used interchangeably in the past, the current "emphasis is on account data throughout the standard, possibly acknowledging that individuals" are not exclusively cardholders any longer. This emphasizes the necessity to exercise caution & prudence when determining the applicability of PCI-DSS.

Version 3.2.1 states that PCI-DSS requirements apply to:

Licensed Under Creative Commons Attribution CC BY

"Organisations where account data (cardholder data and/or sensitive authentication data) is stored processed or transmitted."[2]
Version 4.0 states that the requirements apply to:
"Entities with environments where account data (cardholder data and/or sensitive authentication data) is stored, processed, or transmitted, & entities with environments that can impact the security of the Cardholder Data Environment (CDE)."[2]

In contrast to the ISO 27001 Annex A controls, the core framework of PCI-DSS remains unchanged, comprising 12 fundamental obligations that must be fulfilled. However, the phrasing of the standard has undergone considerable alteration & enhancement.

The "Reserve Bank of India has an exhaustive checklist for banks & NBFCs" in India to follow & comply with the RBI-ISMS regulations. The "checklist is fashioned to target even the smallest of assets & find every" security loophole. [3] This motivated the researcher to research the latest updates to ISO & PCI-DSS to determine the robustness of both together.

2. The Benefits & Challenges of PCI-DSS Compliance

The Payment Card Industry Data Security Standard (PCI-DSS) is a set of security standards created to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. Here are some of the benefits & challenges of PCI-DSS:

2.1 Benefits

- **Reduced risk of data breaches:** Implementing the PCI-DSS helps reduce the risk of data breaches, which can result in significant financial & reputational damage to a company.
- **Increased customer trust:** Compliance with PCI-DSS standards can help increase customer trust, as they know their payment card data is being handled securely.
- **Legal compliance:** Many countries have laws & regulations that require companies to protect sensitive data, including payment card data. Compliance with PCI-DSS can help companies meet these requirements.
- **Better overall security:** PCI-DSS is a comprehensive set of security standards that cover everything from network security to employee training. Implementing these standards can help companies improve their overall security posture.
- **Cost savings:** While implementing PCI-DSS may require an initial investment in technology & personnel, it can ultimately save companies money by reducing the risk of data breaches & associated costs.

Figure 4: Benefits of PCI-DSS compliance

2.2 Challenges

- **Complexity:** The PCI-DSS standard is complex & can be difficult to understand & implement for some organizations.
- **Cost:** Implementing the necessary technology & personnel to achieve PCI-DSS compliance can be expensive, especially for smaller organizations.
- **Continuous monitoring:** Achieving compliance is not a one-time event but an ongoing process that requires continuous monitoring & maintenance.
- **Resource-intensive:** Achieving & maintaining PCI-DSS compliance can be resource-intensive, requiring significant time & effort from IT & security teams.
- **Non-compliance penalties:** Non-compliance with PCI-DSS can result in significant fines & penalties, as well as damage to a company's reputation.

Figure 5: Challenges of PCI-DSS compliance

3. Similarities & Differences between ISO 27001 & PCI-DSS

3.1 Mapping of PCI-DSS requirements to ISO/IEC 27001

The PCI-DSS is a comprehensive set of technical & operational requirements that form a baseline for protecting account data. The requirements are organized into twelve categories, which collectively comprise nearly 200 security controls. Notably, this research article includes an "**Annexure A**" that presents a mapping of PCI-DSS requirements to the ISO/IEC 27001 standard. This mapping serves as a valuable resource for organizations seeking to achieve compliance with both standards & ensures that their security controls satisfy the requirements of both frameworks. As such, organizations seeking to attain compliance with PCI-DSS & ISO/IEC 27001 are encouraged to refer to "Annexure A" for guidance & reference.

Licensed Under Creative Commons Attribution CC BY

3.2 Gap Analysis

The Payment Card Industry Data Security Standard (PCI-DSS) & the International Organization for Standardization's (ISO) 27001 standard are both concerned with safeguarding data through technical & organizational controls. However, there are differences in their approaches, as PCI-DSS adopts a more prescriptive rule-based approach, while ISO 27001 is based on a risk management framework. PCI-DSS provides a baseline for securing payment card data, while ISO 27001 provides a broader framework for information security management.

ISO 27001 has a crucial feature called PDCA (Plan, Do, Check, Act) that is not present in PCI-DSS. PDCA is a standard management system approach that is part of any ISO-based management system. Consequently, ISO 27001 is a better choice for organizations that already have a management system & want to improve their information security or for those that lack a management system & want to safeguard their information. On the other hand, PCI-DSS is mandatory for organizations that deal with credit card transactions & is the more appropriate choice in such cases.

Category	PCI-DSS	ISO 27001
Flexibility	Very low	Very high
Scope	Account data	Depends on the organization
Control Requirements	Prescriptive & well defined	High-level & risk-based
Direction	'Must' apply the control	Inclusion/exclusion is determined by risk

Figure 6: Comparison between PCI-DSS & ISO 27001

4. Implementation

The ISO/IEC 27001 standard presents a structured & comprehensive framework for handling information security matters within an organization. It entails a methodical approach to identifying, evaluating, & addressing risks to the confidentiality, integrity, & accessibility of the organization's information assets. Combining & incorporating both standards can offer a significant competitive advantage, as it allows for the implementation of a management system alongside generic security controls & tailored controls for credit card environments. Furthermore, the integration process is relatively straight forward since many controls of both standards share similarities. Consequently, it can be a favourable prospect for an enterprise that deals with credit card data & aspires to establish a management system for strategically planning, implementing, reviewing, & enhancing security controls to consider the joint implementation of PCI-DSS & ISO 27001. The adoption of ISO/IEC 27001 assists in fulfilling numerous PCI-DSS prerequisites & leads to an overall improvement in the organization's information security position.

5. Working with PCI-DSS & ISO 27001 Together Using Gap Analysis

In the context of PCI-DSS compliance, implementing ISO/IEC 27001 can help the financial institution to meet several requirements of the standard, such as:

- **Risk assessment & management:** PCI-DSS requires organizations to conduct regular risk assessments & implement measures to manage identified risks. ISO/IEC 27001 provides a framework for conducting risk assessments & implementing risk management controls.
- **Information security policies:** PCI-DSS requires organizations to have documented information security policies that address various aspects of information security. ISO/IEC 27001 provides a framework for developing, implementing, & maintaining such policies.
- **Access control:** PCI-DSS requires organizations to restrict access to cardholder data to authorized personnel. ISO/IEC 27001 provides a framework for implementing access control measures, such as user authentication & authorization, to protect sensitive information.
- **Incident management:** PCI-DSS requires organizations to have an incident response plan to address security incidents. ISO/IEC 27001 provides a framework for developing & implementing incident management procedures to detect, assess, & respond to security incidents. [4]

6. Benefits of Implementing an Integrated Model of PCI-DSS & ISO/IEC 27001

- **Aligning with best practices:** ISO 27001 is a widely recognized international standard for "information security management. It provides a framework for establishing, implementing, maintaining, & continually improving" an ISMS. By implementing ISO 27001, organizations can ensure that their PCI-DSS compliance efforts are aligned with internationally recognized best practices for information security.
- **A comprehensive approach to security:** While PCI-DSS focuses on protecting payment card data, ISO 27001 takes a more comprehensive approach to information security, covering all types of information assets. By implementing ISO 27001, organizations can ensure that all of their information assets are protected from a wide range of security threats.
- **Continuous improvement:** ISO 27001 requires organizations to continually monitor & improve their ISMS to ensure that it remains effective over time. By implementing ISO 27001, organizations can ensure that their PCI-DSS compliance efforts remain up-to-date & effective in the face of evolving security threats.
- **Third-party validation:** ISO 27001 certification provides a way for organizations to demonstrate their commitment to information security best practices to stakeholders. This can include customers, partners, & regulators who may be concerned about the security of their information. By obtaining ISO 27001 certification, organizations can demonstrate that they have implemented a comprehensive approach to information security that is regularly audited by a third-party certification body. [4]

7. Case Study: XYZ Organisation

One example of an organization that has implemented both PCI-DSS & ISO 27001 is XYZ organisation. XYZ org., a global online payments company, is required to comply with

Licensed Under Creative Commons Attribution CC BY

both PCI-DSS & ISO 27001 due to the sensitive financial information it handles.

To comply with PCI-DSS, XYZ org. implemented a range of security controls such as data encryption, access controls, & regular security testing. However, XYZ org. recognized that PCI-DSS alone could not provide comprehensive security for its financial information, & decided to implement ISO 27001 to complement its PCI-DSS compliance efforts.

XYZ org. 's ISO 27001 implementation included a thorough risk assessment, the development of an information security policy, & the implementation of a comprehensive set of security controls across the organization. The company also established ISMS to manage its security program & ensure ongoing compliance with ISO 27001. [4]

7.1 Challenges XYZ Organisation Faces when Implementing both Standards

- **Resource allocation:** Implementing both standards requires significant resources, including time, money, & personnel. Organizations need to ensure they have sufficient resources to effectively implement & maintain both standards.
- **Conflicting requirements:** PCI-DSS & ISO 27001 have different requirements & priorities, which can sometimes conflict with each other. Organizations need to carefully analyse these requirements & identify areas where there may be conflicts, so they can develop a strategy to address them.
- **Complexity:** Combining two complex standards can create additional complexity for organizations, which can make it more difficult to maintain compliance. Organizations need to ensure they have a clear understanding of both standards & how they work together & develop a strategy for managing this complexity.
- **Maintenance:** Both standards require ongoing monitoring, testing, & maintenance to ensure ongoing compliance. Organizations need to have a clear plan for maintaining both standards, including regular reviews & updates to security controls & policies.
- **Geographic reach:** XYZ org. operates in numerous countries worldwide, each with its own set of regulatory requirements. Complying with both standards across all these jurisdictions can be a significant challenge.

7.2 Benefits XYZ Organization gets by Complying with both PCI-DSS & ISO 27001

- **Improved compliance:** By complying with both PCI-DSS & ISO 27001, XYZ org. was able to demonstrate a commitment to information security & achieve compliance with two internationally recognized standards.
- **Better risk management:** The combination of PCI-DSS & ISO 27001 allowed XYZ org. to identify & mitigate potential security risks more effectively, helping to prevent data breaches & other security incidents.
- **Increased efficiency:** The implementation of an ISMS helped XYZ org. improve the overall efficiency & effectiveness of its security program, reducing the time & effort required to manage security-related tasks.
- **Enhanced reputation & customer:** By implementing two robust & widely recognized security standards, XYZ org. was able to enhance its reputation & demonstrate its commitment to protecting customer information.

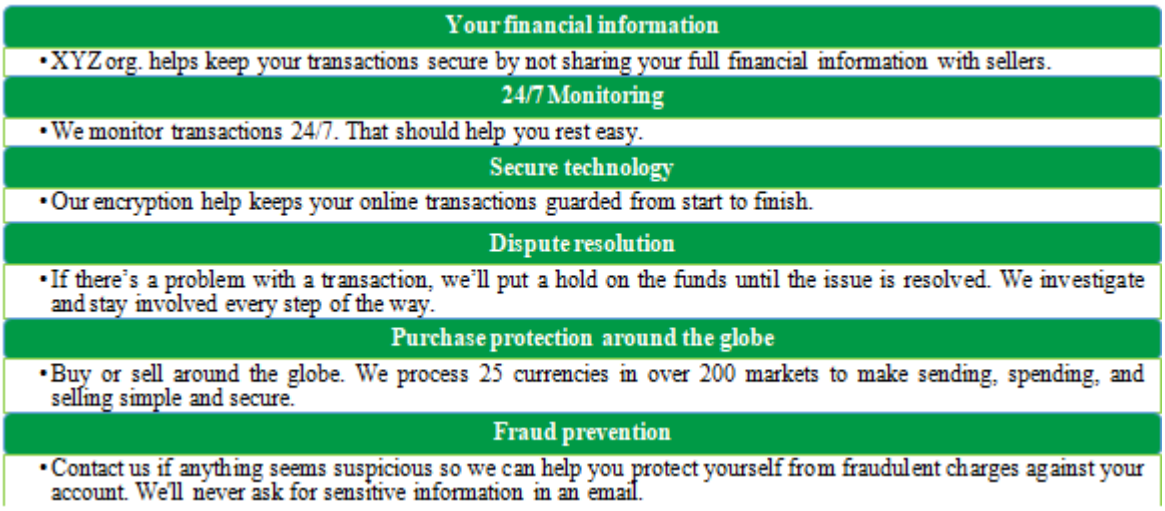

Figure 7: Security for buyers

Cost savings: By implementing a comprehensive security program that complies with both standards, XYZ org. was able to reduce the risk of costly security incidents & improve the efficiency of its security program, potentially resulting in cost savings over time.

7.3 Conclusion of Case Study

Implementing ISO 27001 alongside PCI-DSS, XYZ org. was able to achieve a more holistic approach to information security. The combination of the two standards helped the company identify & mitigate potential security risks more effectively, as well as improve the overall efficiency & effectiveness of its security program.

Licensed Under Creative Commons Attribution CC BY

8. Certification Schemes

Certification is a crucial step following the adoption of standards, & it should be noted that the certification processes for ISO 27001 & SOC 2 are distinct from each other. Specifically, ISO 27001 certification is overseen by the International Organization for Standardization (ISO), which consists of members from around the globe. Certification is performed by accredited certification bodies, which in turn are accredited by national accreditation bodies. Furthermore, each certification body requires its auditors to meet certain qualifications.

With regards to PCI-DSS, the PCI-SSC serves as the central governing body. The council consists of the most significant payment processing entities, namely Visa, MasterCard, American Express, Discover Financial Services, & JCB International. However, it should be noted that the PCI-SSC does not oversee compliance with the PCI-DSS standard; rather, this responsibility falls on each respective brand. To this end, a Qualified Security Assessor (QSA), who has been approved by the PCI-SSC, is appointed to generate a Report on Compliance (ROC) for companies that process significant volumes of transactions. Conversely, companies that handle lower transaction values are required to complete a Self-Assessment Questionnaire (SAQ). [5]

9. Conclusion

After analysis of the PCI-DSS v4.0 & ISO 27001: 2022 standards, it is evident that they both provide a comprehensive approach to information security management. While PCI-DSS primarily focuses on securing payment card data, ISO 27001 provides a broader framework for managing information security risks for all types of information assets. Integrating both standards can differentiate an organization by aligning its information security efforts with internationally recognized best practices & ensuring continuous improvement, while also providing third-party validation.

However, careful planning & significant resources are necessary to implement both standards & organizations should assess their information security needs & resources before proceeding. It is essential to note that compliance with standards does not guarantee complete security, & regular monitoring & assessment of information security controls is necessary.

The XYZ org. case study demonstrates that organizations can successfully implement both standards to enhance their information security posture. Ultimately, a comprehensive security framework built on ISO 27001: 2022 & PCI-DSS v4.0 can significantly enhance an organization's security posture & provide customers with confidence in the security of their data.

Note: In this research article, the researcher has provided a mapping of PCI DSS v4.0 requirements to ISO 27001: 2022 in **Annexure A** for organizational reference. It is important to note that this mapping is based on the researcher's understanding, & variations may occur depending on the reader's perspective.

10. Suggestions

- Organizations should carefully assess their information security needs & resources before deciding to implement both PCI-DSS & ISO 27001.
- Conduct a careful assessment of information security needs & resources before deciding to implement both standards to ensure adequate planning & resource allocation.
- Ensure that information security policies & procedures are regularly reviewed & updated to align with changing threats & best practices.
- Provide regular training & awareness programs to all employees on information security best practices & policies to promote a culture of security.

11. Scope of Future Research

The researcher was unable to research the elements listed below due to a lack of resources & time, despite their high research potential. However, the reader is encouraged to do so if they so desire.

- A comparative study of other standards & frameworks for information security management, & their compatibility with PCI-DSS & ISO 27001.
- An analysis of the potential cost-benefit trade-offs associated with implementing both standards & the factors that influence the decision-making process.
- An examination of the role of training & awareness programs in ensuring successful implementation & adoption of both standards.

References

[1] Tripwire, 'PCI-DSS 4.0 and ISO 27001 - the dynamic duo' (27 April 2022) <https://www.tripwire.com/state-of-security/pci-dss-4-0-iso-27001-dynamic-duo> accessed 4 April 2023.
[2] Goodspeed L, 'Updated PCI-DSS v4.0 Timeline' (*PCI Security Standards*, 17 June 2021)<https://blog.pcisecuritystandards.org/updated-pci-dss-v4.0-timeline> accessed 4 April 2023.
[3] Tagade K, 'ISO 27001 Penetration Testing and Other Pentesting Compliance - A Comprehensive Guide' (*Astra*, 28 February 2023) <https://www.getastra.com/blog/security-audit/iso-27001-penetration-testing/> accessed 6 April 2023.
[4] Kolochenko I N, 'Stop data breaches with ISO 27001' (*BCS*, 3 August 2021) <https://www.bcs.org/articles-opinion-and-research/stop-data-breaches-with-iso-27001 /> accessed 9 April 2023.
[5] Antonio Jose Segovia, 'PCI-DSS vs. ISO 27001: Similarities, differences, implementation, and certification' (*Advisera*)<https://advisera.com/27001academy/knowledgebase/pci-dss/> accessed 4 April 2023.

Licensed Under Creative Commons Attribution CC BY

Author Profile

Adesh Mukati, Student, Master of Cyber Law and Information Security, National Law Institute University, Bhopal. Adesh Mukati is a 1st year student of Master of Cyber Law and Information Security at NLIU, Bhopal, and completed his undergrad in Biochemistry from Govt. Motilal Vigyan Mahavidyalaya, Bhopal. He is a highly motivated individual who is diligently working towards securing a challenging position in a reputable organization. He aims to expand his learning, knowledge, and skills and further develop his professional capabilities. With a strong work ethic and dedication to his career, he is eager to make a valuable contribution to any organization that he joins.

Dr. Astitwa Bhargava, Assistant Professor and Placement Coordinator, Department of Cyber Law and Information Security, Rajiv Gandhi National Cyber Law Centre, National Law Institute University, Bhopal. Astitwa Bhargava has obtained his Ph.D. in Cyber Law and Information Security from the National Law University, Jodhpur. He also holds M.S. in Cyber Law and Information Security from the National Law Institute University, Bhopal and B.E. in Computer Science from R.G.P.V, Bhopal. He has successfully completed certifications like CDPSE, CTPRP, CCSK, OneTrust Privacy Management Professional, OneTrust Expert Certifications, and BigID Privacy Management Professional. He has more than 9 years of teaching and corporate experience. Prior joining to NLIU Bhopal in January, 2022, he was working as an Assistant Manager, Consulting at KPMG, Bangalore. Astitwa's research and teaching interests are in the area of Data Privacy and Protection, Information Security Compliances (ISO 27001:2013, NIST 800-53, NIST CSF, HIPAA, etc.), Business Continuity Planning and Disaster Recovery Planning. He has published various research papers in the National and International forums on Data Privacy and Protection, various information security compliances, e-commerce security, BYOD, and Big Data. He has also presented number of research papers in the International and National Conferences.

Annexure A: Mapping of PCI DSS v4.0 Requirements to ISO 27001: 2022

S. No.	PCI-DSS v4.0 Clauses	PCI-DSS v.4.0 Requirement	PCI-DSS v4.0 Control	PCI DSS v4.0 Control Titles	ISO/IEC 27001: 2013 Controls	ISO/IEC 27001: 2022 Clauses	ISO/IEC 27001: 2022 Controls	ISO/IEC 27001: 2022 Control Titles
1.	Build & Maintain a Secure Network & Systems	Install & maintain network security controls	1.1.1	Security policies & operational procedures must be: Documented, up-to-date, in use, & known to all parties.	A.12.1.1	Operations Security	A.5.37	Documented operating procedures
			6.5.1	System changes follow established procedures, including documentation, approval, & testing.	A.12.1.2 A.14.2.2 A.14.2.3 A.14.2.4		A.8.32	Change management
			2.2.4	Selective enabling & disabling of necessary services & functionality.	A.12.1.3		A.8.6	Capacity management
			6.5.3	Pre-production environments are separated from production environments & the separation is enforced with access controls.	A.12.1.4		A.8.31	Separation of development, test, & operational environments
			5.2.1	Anti-malware deployed on all components, except non-vulnerable ones.	A.12.2.1		A.8.7	Protection against malware
			9.4.1.1	Offline media backups with cardholder data are stored in a secure location.	A.12.3.1		A.8.13	Information backup
			9.4.1.2	The security of the offline media backup location (s) with cardholder data is reviewed at least once every 12 months.				No Map
			10.4.1	Audit logs reviewed daily: security events, CHD/SAD, critical components, security functions.	A.12.4.1		A.8.15	Logging
			10.4.2	Logs of all other system components (those not specified in Requirement 10.4.1) are reviewed periodically.				
			10.4.1	Daily review: security events, CHD/SAD, critical components, security functions.			A.8.16	Monitoring activities
			10.6.1	System clocks & time are synchronized using time-synchronization technology.	A.12.4.4		A.8.17	Clock Synchronization
			12.2.1	End-user technology policies: approved use, authorized parties, approved products.	A.12.5.1		A.8.19	Installation of software on operational systems
			6.3	Security vulnerabilities are identified & addressed.	A.12.6.1		A.8.8	Management of technical vulnerabilities
			2.1	Processes & mechanisms for applying secure configurations to all system components are defined & understood.			A.8.9	Configuration management
			2.2	System components are configured & managed securely.				
			2.3	Wireless environments are configured & managed securely.				

Licensed Under Creative Commons Attribution CC BY

			3.2.1	Account data storage: retention, disposal, coverage, secure deletion, verification.			A.8.10	Information deletion
			3.4.1	PAN masking: limited display to authorized personnel, BIN & last four digits.			A.8.11	Data masking
			A3.2.6	Prevention of cleartext PAN leakage: active detection, logging, & alerts.			A.8.12	Data leakage prevention
			10.4.3	Exceptions & anomalies identified during the review process are addressed.	A.12.7.1		A.8.34	Protection of information systems during audit testing
			10.4.1.1	Automated mechanisms are used to perform audit log reviews.				
			4.1.1	Policies & procedures documented, updated, used, & known.	A.13.2.1 A.13.2.2 A.13.2.3	Communications Security	A.5.14	Information transfer
			3.1.1	Documented, updated, used, known security policies & procedures.	A.13.2.4		A.6.6	Confidentiality or non-disclosure agreements
			1.2.1	NSC ruleset configuration standards: defined, implemented, maintained.	A.13.1.1		A.8.20	Networks security
			1.4	Network connections between trusted & untrusted networks are controlled.	A.13.1.2		A.8.21	Security of network services
			1.2.1	NSC ruleset configuration standards: defined, implemented, maintained.	A.13.1.3		A.8.22	Segregation of networks
			5.4.1	Processes & automated mechanisms are in place to detect & protect personnel against phishing attacks.			A.8.23	Web filtering
.		Apply secure configurations to all system components	1.1.1	Verification of Requirement 1: Policies & procedures management assessment.	A.12.1.1	Operations Security	A.5.37	Documented operating procedures
			6.5.1	System component changes follow established procedures, including documentation, approval, testing.	A.12.1.2 A.14.2.2 A.14.2.3 A.14.2.4		A.8.32	Change management
			2.2.4	Selective enabling & disabling of necessary services & functionality.	A.12.1.3		A.8.6	Capacity management
			6.5.3	Pre-production environments are separated from production environments & the separation is enforced with access controls.	A.12.1.4		A.8.31	Separation of development, test & production environments
			5.2.1	Anti-malware deployed on all components, except non-vulnerable ones.	A.12.2.1		A.8.7	Protection against malware
			9.4.1.1	Offline media backups with cardholder data are stored in a secure location.	A.12.3.1		A.8.13	Information backup
			9.4.1.2	The security of the offline media backup location (s) with cardholder data is reviewed at least once every 12 months.				No Map
			10.4.1	Audit logs reviewed daily: security events, CHD/SAD, critical components, security functions.	A.12.4.1		A.8.15	Logging
			10.4.2	Logs of all other system components (those not specified in Requirement 10.4.1) are reviewed periodically.				
			10.4.1	Audit logs reviewed daily: security events, CHD/SAD, criticalcomponents, security functions.			A.8.16	Monitoring activities
			10.6.1	System clocks & time are synchronized using time-synchronization technology.	A.12.4.4		A.8.17	Clock synchronization
			12.2.1	End-user technology policies: approved use, authorized parties, approved products.	A.12.5.1		A.8.19	Installation of software on operational system
			6.3	Security vulnerabilities are identified & addressed.	A.12.6.1		A.8.8	Management of technical vulnerabilities
			2.1	Processes & mechanisms for applying secure configurations to all system components are defined & understood.			A.8.9	Configuration management
			2.2	System components are configured & managed securely.				
			2.3	Wireless environments are configured &				

Licensed Under Creative Commons Attribution CC BY

				managed securely.				
			3.2.1	Account data storage: retention, disposal, coverage, secure deletion, verification.			A.8.10	Information deletion
			3.4.1	PAN masking: limited display to authorized personnel, BIN & last four digits.			A.8.11	Data masking
			A3.2.6	Prevention of cleartext PAN leakage: active detection, logging, & alerts.			A.8.12	Data leakage prevention
			10.4.3	Exceptions & anomalies identified during the review process are addressed.	A.12.7.1		A.8.34	Protection of information systems during audit testing
			10.4.1.1	Automated mechanisms are used to perform audit log reviews.				
			4.1.1	Policies & procedures documented, updated, used, & known.	A.13.2.1 A.13.2.2 A.13.2.3	Communications Security	A.5.14	Information transfer
			3.1.1	Documented, updated, used, known security policies & procedures.	A.13.2.4		A.6.6	Confidentiality or non-disclosure agreements
			1.2.1	NSC ruleset configuration standards: defined, implemented, maintained.	A.13.1.1		A.8.20	Networks security
			1.4	Network connections between trusted & untrusted networks are controlled.	A.13.1.2		A.8.21	Security of network services
			1.2.1	NSC ruleset configuration standards: defined, implemented, maintained.	A.13.1.3		A.8.22	Segregation of networks
			5.4.1	Processes & automated mechanisms are in place to detect & protect personnel against phishing attacks.			A.8.23	Web filtering
.	Protect **account**Data	Protect stored account data	1.1.1	Security policies & operational procedures must be: Documented, up-to-date, in use, & known to all parties.	A.12.1.1	Operations Security	A.5.37	Documented operating procedures
			6.5.1	System changes follow established procedures, including documentation, approval, & testing.	A.12.1.2 A.14.2.2 A.14.2.3 A.14.2.4		A.8.32	Change management
			2.2.4	Selective enabling & disabling of necessary services & functionality.	A.12.1.3		A.8.6	Capacity management
			6.5.3	Pre-production environments are separated from production environments & the separation is enforced with access controls.	A.12.1.4		A.8.31	Separation of development, test, & operational environments
			5.2.1	Anti-malware deployed on all components, except non-vulnerable ones.	A.12.2.1		A.8.7	Protection against malware
			9.4.1.1	Offline media backups with cardholder data are stored in a secure location.	A.12.3.1		A.8.13	Information backup
			9.4.1.2	The security of the offline media backup location (s) with cardholder data is reviewed at least once every 12 months.				No Map
			10.4.1	Audit logs reviewed daily: security events, CHD/SAD, critical components, security functions.	A.12.4.1		A.8.15	Logging
			10.4.2	Logs of all other system components (those not specified in Requirement 10.4.1) are reviewed periodically.				
			10.4.1	Audit logs reviewed daily: security events, CHD/SAD, critical components, security functions.			A.8.16	Monitoring activities
			10.6.1	System clocks & time are synchronized using time-synchronization technology.	A.12.4.4		A.8.17	Clock Synchronization
			12.2.1	End-user technology policies: approved use, authorized parties, approved products.	A.12.5.1		A.8.19	Installation of software on operational systems
			6.3	Security vulnerabilities are identified & addressed.	A.12.6.1		A.8.8	Management of technical vulnerabilities
			2.1	Processes & mechanisms for applying secure configurations to all system components are defined & understood.			A.8.9	Configuration management
			2.2	System components are configured & managed securely.				

Licensed Under Creative Commons Attribution CC BY

			2.3	Wireless environments are configured & managed securely.				
			3.2.1	Account data storage: retention, disposal, coverage, secure deletion, verification.			A.8.10	Information detection
			3.4.1	PAN masking: limited display to authorized personnel, BIN & last four digits.			A.8.11	Data masking
			A3.2.6	Prevention of cleartext PAN leakage: active detection, logging, & alerts.			A.8.12	Data leakage prevention
			10.4.3	Exceptions & anomalies identified during the review process are addressed.	A.12.7.1		A.8.34	Protection of information systems during audit testing
			10.4.1.1	Automated mechanisms are used to perform audit log reviews.				
			4.1.1	Policies & procedures documented, updated, used, & known.	A.13.2.1 A.13.2.2 A.13.2.3	Communications Security	A.5.14	Information transfer
			3.1.1	Documented, updated, used, known security policies & procedures.	A.13.2.4		A.6.6	Confidentiality or non-disclosure agreements
			1.2.1	NSC ruleset configuration standards: defined, implemented, maintained.	A.13.1.1		A.8.20	Networks security
			1.4	Network connections between trusted & untrusted networks are controlled.	A.13.1.2		A.8.21	Security of network services
			1.2.1	NSC ruleset configuration standards: defined, implemented, maintained.	A.13.1.3		A.8.22	Segregation of networks
			5.4.1	Processes & automated mechanisms are in place to detect & protect personnel against phishing attacks.			A.8.23	Web filtering
		Protect cardholder data with strong cryptography during transmission over open, public networks	6.4.1	Public-facing web applications: vulnerability assessment or automated attack prevention.	A.14.1.2	System Acquisition, Development, & Maintenance	A.8.26	Application security requirements
			6.2.1	Secure development: industry standards, PCI DSS, throughout software lifecycle.	A.14.2.1		A.8.25	Secure development life cycle
			6.1	Processes & mechanisms for developing & maintaining secure systems & software are defined & understood.	A.14.2.5		A.8.27	Secure system architecture & engineering principles
			6.2.3	Software review: code adherence, vulnerability identification, corrective implementation before release.			A.8.28	Secure coding
			6.2.3	Software review: code adherence, vulnerability identification, corrective implementation before release.	A.14.2.8		A.8.29	Security testing in development & acceptance
			6.2.3	Software review: code adherence, vulnerability identification, corrective implementation before release.	A.14.2.7		A.8.30	Outsourced development
			6.5.6	Test data & test accounts are removed from system components before the system goes into production.	A.14.3.1		A.8.33	Test information
	Maintain a Vulnerability Management Program	Protect all systems & networks from malicious software	6.4.1	Public-facing web applications: vulnerability assessment or automated attack prevention.	A.14.1.2	System Acquisition, Development, & Maintenance	A.8.26	Application security requirements
			6.2.1	Secure development: industry standards, PCI DSS, throughout software lifecycle.	A.14.2.1		A.8.25	Secure development life cycle
			6.1	Processes & mechanisms for developing & maintaining secure systems & software are defined & understood.	A.14.2.5		A.8.27	Secure system architecture & engineering principles
			6.2.3	Software review: code adherence, vulnerability identification, corrective implementation before release.			A.8.28	Secure coding
			6.2.3	Software review: code adherence, vulnerability identification, corrective implementation before release.	A.14.2.8		A.8.29	Security testing in development & acceptance
			6.2.3	Software review: code adherence, vulnerability identification, corrective implementation before release.	A.14.2.7		A.8.30	Outsourced development

Licensed Under Creative Commons Attribution CC BY

			6.5.6	Test data & test accounts are removed from system components before the system goes into production.	A.14.3.1		A.8.33	Test information
.		Develop & maintain secure systems & software	6.4.1	Public-facing web applications: vulnerability assessment or automated attack prevention.	A.14.1.2	System Acquisition, Development, & Maintenance	A.8.26	Application security requirements
			6.2.1	Secure development: industry standards, PCI DSS, throughout software lifecycle.	A.14.2.1		A.8.25	Secure development life cycle
			6.1	Processes & mechanisms for developing & maintaining secure systems & software are defined & understood.	A.14.2.5		A.8.27	Secure system architecture & engineering principles
			6.2.3	Software review: code adherence, vulnerability identification, corrective implementation before release.			A.8.28	Secure coding
			6.2.3	Software review: code adherence, vulnerability identification, corrective implementation before release.	A.14.2.8		A.8.29	Security testing in development & acceptance
			6.2.3	Software review: code adherence, vulnerability identification, corrective implementation before release.	A.14.2.7		A.8.30	Outsourced development
			6.5.6	Test data & test accounts are removed from system components before the system goes into production.	A.14.3.1		A.8.33	Test information
.	Implement Strong Access Control Measures	Restrict access to system components & cardholder data by business need to know	1.1.1	Security policies & operational procedures must be: Documented, up-to-date, in use, & known to all parties.	A.12.1.1	Operations Security	A.5.37	Documented operating procedures
			6.5.1	System changes follow established procedures, including documentation, approval, & testing.	A.12.1.2 A.14.2.2 A.14.2.3 A.14.2.4		A.8.32	Change management
			2.2.4	Selective enabling & disabling of necessary services & functionality.	A.12.1.3		A.8.6	Capacity management
			6.5.3	Pre-production environments are separated from production environments & the separation is enforced with access controls.	A.12.1.4		A.8.31	Separation of development, test, & operational environments
			5.2.1	Anti-malware deployed on all components, except non-vulnerable ones.	A.12.2.1		A.8.7	Protection against malware
			9.4.1.1	Offline media backups with cardholder data are stored in a secure location.	A.12.3.1		A.8.13	Information backup
			9.4.1.2	The security of the offline media backup location (s) with cardholder data is reviewed at least once every 12 months.				No Map
			10.4.1	Audit logs reviewed daily: security events, CHD/SAD, critical components, security functions.	A.12.4.1		A.8.15	Logging
			10.4.2	Logs of all other system components (those not specified in Requirement 10.4.1) are reviewed periodically.				
			10.4.1	Audit logs reviewed daily: security events, CHD/SAD, critical components, security functions.			A.8.16	Monitoring activities
			10.6.1	System clocks & time are synchronized using time-synchronization technology.	A.12.4.4		A.8.17	Clock Synchronization
			12.2.1	End-user technology policies: approved use, authorized parties, approved products.	A.12.5.1		A.8.19	Installation of software on operational systems
			6.3	Security vulnerabilities are identified & addressed.	A.12.6.1		A.8.8	Management of technical vulnerabilities
			2.1	Processes & mechanisms for applying secure configurations to all system components are defined & understood.			A.8.9	Configuration management
			2.2	System components are configured & managed securely.				
			2.3	Wireless environments are configured & managed securely.				

Licensed Under Creative Commons Attribution CC BY

			3.2.1	Account data storage: retention, disposal, coverage, secure deletion, verification.			A.8.10	Information detection
			3.4.1	PAN masking: limited display to authorized personnel, BIN & last four digits.			A.8.11	Data masking
			A3.2.6	Prevention of cleartext PAN leakage: active detection, logging, & alerts.			A.8.12	Data leakage prevention
			10.4.3	Exceptions & anomalies identified during the review process are addressed.	A.12.7.1		A.8.34	Protection of information systems during audit testing
			10.4.1.1	Automated mechanisms are used to perform audit log reviews.				
			4.1.1	Policies & procedures documented, updated, used, & known.	A.13.2.1 A.13.2.2 A.13.2.3	Communications Security	A.5.14	Information transfer
			3.1.1	Documented, updated, used, known security policies & procedures.	A.13.2.4		A.6.6	Confidentiality or non-disclosure agreements
			1.2.1	NSC ruleset configuration standards: defined, implemented, maintained.	A.13.1.1		A.8.20	Networks security
			1.4	Network connections between trusted & untrusted networks are controlled.	A.13.1.2		A.8.21	Security of network services
			1.2.1	NSC ruleset configuration standards: defined, implemented, maintained.	A.13.1.3		A.8.22	Segregation of networks
			5.4.1	Processes & automated mechanisms are in place to detect & protect personnel against phishing attacks.			A.8.23	Web filtering
.		Identify users & authenticate access to system components	1.1.1	Security policies & operational procedures must be: Documented, up-to-date, in use, & known to all parties.	A.12.1.1	Operations Security	A.5.37	Documented operating procedures
			6.5.1	System changes follow established procedures, including documentation, approval, & testing.	A.12.1.2 A.14.2.2 A.14.2.3 A.14.2.4		A.8.32	Change management
			2.2.4	Selective enabling & disabling of necessary services & functionality.	A.12.1.3		A.8.6	Capacity management
			6.5.3	Pre-production environments are separated from production environments & the separation is enforced with access controls.	A.12.1.4		A.8.31	Separation of development, test, & operational environments
			5.2.1	Anti-malware deployed on all components, except non-vulnerable ones.	A.12.2.1		A.8.7	Protection against malware
			9.4.1.1	Offline media backups with cardholder data are stored in a secure location.	A.12.3.1		A.8.13	Information backup
			9.4.1.2	The security of the offline media backup location (s) with cardholder data is reviewed at least once every 12 months.				No Map
			10.4.1	Audit logs reviewed daily: security events, CHD/SAD, critical components, security functions.	A.12.4.1		A.8.15	Logging
			10.4.2	Logs of all other system components (those not specified in Requirement 10.4.1) are reviewed periodically.				
			10.4.1	Audit logs reviewed daily: security events, CHD/SAD, critical components, security functions.			A.8.16	Monitoring activities
			10.6.1	System clocks & time are synchronized using time-synchronization technology.	A.12.4.4		A.8.17	Clock Synchronization
			12.2.1	End-user technology policies: approved use, authorized parties, approved products.	A.12.5.1		A.8.19	Installation of software on operational systems
			6.3	Security vulnerabilities are identified & addressed.	A.12.6.1		A.8.8	Management of technical vulnerabilities
			2.1	Processes & mechanisms for applying secure configurations to all system components are defined & understood.			A.8.9	Configuration management
			2.2	System components are configured & managed securely.				
			2.3	Wireless environments are configured &				

Licensed Under Creative Commons Attribution CC BY

				managed securely.				
			3.2.1	Account data storage: retention, disposal, coverage, secure deletion, verification.			A.8.10	Information detection
			3.4.1	PAN masking: limited display to authorized personnel, BIN & last four digits.			A.8.11	Data masking
			A3.2.6	Prevention of cleartext PAN leakage: active detection, logging, & alerts.			A.8.12	Data leakage prevention
			10.4.3	Exceptions & anomalies identified during the review process are addressed.	A.12.7.1		A.8.34	Protection of information systems during audit testing
			10.4.1.1	Automated mechanisms are used to perform audit log reviews.				
			4.1.1	Policies & procedures documented, updated, used, & known.	A.13.2.1 A.13.2.2 A.13.2.3	Communications Security	A.5.14	Information transfer
			3.1.1	Documented, updated, used, known security policies & procedures.	A.13.2.4		A.6.6	Confidentiality or non-disclosure agreements
			1.2.1	NSC ruleset configuration standards: defined, implemented, maintained.	A.13.1.1		A.8.20	Networks security
			1.4	Network connections between trusted & untrusted networks are controlled.	A.13.1.2		A.8.21	Security of network services
			1.2.1	NSC ruleset configuration standards: defined, implemented, maintained.	A.13.1.3		A.8.22	Segregation of networks
			5.4.1	Processes & automated mechanisms are in place to detect & protect personnel against phishing attacks.			A.8.23	Web filtering
.		Restrict physical access to cardholder data	9.1.1	Requirement 9: Documented, updated, used, known security policies & procedures.	A.11.11.1	Physical & Environmental Controls	A.7.1	Physical security perimeters
			9.4.1	All media with cardholder data is physically secured.				
			9.2.1	Appropriate facility entry controls are in place to restrict physical access to systems in the CDE.	A.11.1.2		A.7.2	Physical entry
			9.2.4	Access to consoles in sensitive areas is restricted via locking when not in use.	A.11.1.3		A.7.3	Securing offices, rooms & facilities
			9.2.1.1	Physical access monitoring: entry/exit points, tamper protection, data storage.			A.7.4	Physical security monitoring
			9.4.1	All media with cardholder data is physically secured.	A.11.1.4		A.7.5	Protecting against physical & environmental threats
			9.4.1.1	Offline media backups with cardholder data are stored in a secure location.				
			9.2.4	Access to consoles in sensitive areas is restricted via locking when not in use.	A.11.1.5		A.7.6	Working in secure areas
			9.3.1	Physical access management: personnel identification, access changes, revocation, authorized control.				
					A.11.2.9		A.7.7	Clear desk & clear screen
					A.11.2.1		A.7.8	Equipment siting & protection
			9.4.3	Secured media transport: logged, tracked, offsite location details.	A.11.2.6		A.7.9	Security of assets off-premises
			12.5.1	An inventory of system components that are in scope for PCI DSS, including a description of function/use, is maintained & kept current.	A.11.2.2		A.7.11	Supporting utilities
			9.5.1	POI device protection: listing, inspection, personnel training for tampering.	A.11.2.3		A.7.12	Cabling security
			12.5.1	An inventory of system components that are in scope for PCI DSS, including a description of function/use, is maintained & kept current.	A.11.2.4		A.7.13	Equipment maintenance
					A.11.2.7		A.7.14	Secure disposal or re-use of equipment
.	Regularly Monitor &	Log & monitor all	1.1.1	Security policies & operational procedures must be: Documented, up-to-date, in use,	A.12.1.1	Operations Security	A.5.37	Documented operating

Licensed Under Creative Commons Attribution CC BY

	Test Networks	access to system components & cardholder data		& known to all parties.				procedures
			6.5.1	System changes follow established procedures, including documentation, approval, & testing.	A.12.1.2 A.14.2.2 A.14.2.3 A.14.2.4		A.8.32	Change management
			2.2.4	Selective enabling & disabling of necessary services & functionality.	A.12.1.3		A.8.6	Capacity management
			6.5.3	Pre-production environments are separated from production environments & the separation is enforced with access controls.	A.12.1.4		A.8.31	Separation of development, test, & operational environments
			5.2.1	Anti-malware deployed on all components, except non-vulnerable ones.	A.12.2.1		A.8.7	Protection against malware
			9.4.1.1	Offline media backups with cardholder data are stored in a secure location.	A.12.3.1		A.8.13	Information backup
			9.4.1.2	The security of the offline media backup location (s) with cardholder data is reviewed at least once every 12 months.				No Map
			10.4.1	Audit logs reviewed daily: security events, CHD/SAD, critical components, security functions.	A.12.4.1		A.8.15	Logging
			10.4.2	Logs of all other system components (those not specified in Requirement 10.4.1) are reviewed periodically.				
			10.4.1	Audit logs reviewed daily: security events, CHD/SAD, critical components, security functions.			A.8.16	Monitoring activities
			10.6.1	System clocks & time are synchronized using time-synchronization technology.	A.12.4.4		A.8.17	Clock Synchronization
			12.2.1	End-user technology policies: approved use, authorized parties, approved products.	A.12.5.1		A.8.19	Installation of software on operational systems
			6.3	Security vulnerabilities are identified & addressed.	A.12.6.1		A.8.8	Management of technical vulnerabilities
			2.1	Processes & mechanisms for applying secure configurations to all system components are defined & understood.			A.8.9	Configuration management
			2.2	System components are configured & managed securely.				
			2.3	Wireless environments are configured & managed securely.				
			3.2.1	Account data storage: retention, disposal, coverage, secure deletion, verification.			A.8.10	Information detection
			3.4.1	PAN masking: limited display to authorized personnel, BIN & last four digits.			A.8.11	Data masking
			A3.2.6	Prevention of cleartext PAN leakage: active detection, logging, & alerts.			A.8.12	Data leakage prevention
			10.4.3	Exceptions & anomalies identified during the review process are addressed.	A.12.7.1		A.8.34	Protection of information systems during audit testing
			10.4.1.1	Automated mechanisms are used to perform audit log reviews.				
			4.1.1	Policies & procedures documented, updated, used, & known.	A.13.2.1 A.13.2.2 A.13.2.3		A.5.14	Information transfer
			3.1.1	Documented, updated, used, known security policies & procedures.	A.13.2.4		A.6.6	Confidentiality or non-disclosure agreements
			1.2.1	NSC ruleset configuration standards: defined, implemented, maintained.	A.13.1.1	Communications Security	A.8.20	Networks security
			1.4	Network connections between trusted & untrusted networks are controlled.	A.13.1.2		A.8.21	Security of network services
			1.2.1	NSC ruleset configuration standards: defined, implemented, maintained.	A.13.1.3		A.8.22	Segregation of networks
			5.4.1	Processes & automated mechanisms are in place to detect & protect personnel against phishing attacks.			A.8.23	Web filtering
.		Test security	6.4.1	Public-facing web applications:	A.14.1.2	System	A.8.26	Application

Licensed Under Creative Commons Attribution CC BY

		of systems & networks regularly		vulnerability assessment or automated attack prevention.		Acquisition, Development, & Maintenance		security requirements
			6.2.1	Secure development: industry standards, PCI DSS, throughout software lifecycle.	A.14.2.1		A.8.25	Secure development life cycle
			6.1	Processes & mechanisms for developing & maintaining secure systems & software are defined & understood.	A.14.2.5		A.8.27	Secure system architecture & engineering principles
			6.2.3	Software review: code adherence, vulnerability identification, corrective implementation before release.			A.8.28	Secure coding
			6.2.3	Software review: code adherence, vulnerability identification, corrective implementation before release.	A.14.2.8		A.8.29	Security testing in development & acceptance
			6.2.3	Software review: code adherence, vulnerability identification, corrective implementation before release.	A.14.2.7		A.8.30	Outsourced development
			6.5.6	Test data & test accounts are removed from system components before the system goes into production.	A.14.3.1		A.8.33	Test information
			12.1.3	Clear security policy: defined roles, personnel awareness & acknowledgment.	A.6.1.1	Organization of Information	A.5.2	Information security roles & responsibilities
			6.5.4	Separation of roles: production vs. pre-production, reviewed/approved changes deployment.	A.6.1.2		A.5.3	Segregation of duties
			6.5.1	System changes follow established procedures, including documentation, approval, & testing.	A.6.1.3		A.5.5	Contact with authorities
					A.6.1.4		A.5.6	Contact with special interest groups
			12.3.1	Flexible requirement support: documented risk analysis, asset/threat identification, periodic review.			A.5.7	Threat intelligence
					A.6.1.5		A.5.8	Information security in project management
			2.2.7	All non-console administrative access is encrypted using strong cryptography.	A.6.2.2		A.6.7	Remote working
			8.2.3	Additional requirement for service providers only: Service providers with remote access to customer premises use unique authentication factors for each customer premises.				
			8.4.3	MFA for remote network access: personnel & third parties.				
			12.1	A comprehensive information security policy that governs & provides direction for protection of the entity's information assets is known & current.	A.18.1.1 A.18.1.5	Compliance	A.5.31	Legal, statutory, regulatory & contractual requirements
					A.18.1.2		A.5.32	Intellectual property rights
			3.6	Cryptographic keys used to protect stored account data are secured.	A.18.1.3		A.5.33	Protection of records
			3.5.1	PAN is made unreadable using one-way hashes, truncation, index tokens, or strong cryptography with key management processes.	A.18.1.4		A.5.34	Privacy & protection of personal identifiable information (PII)
			1.5.1	Security controls on computing devices: configuration, active, authorized alterations.	A.6.2.1		A.8.1	User end point devices
.	Maintain an Information Security Policy	Support information security within organizational	12.1	A comprehensive information security policy that governs & provides direction for protection of the entity's information assets is known & current.	A.5.1.1	Policies for information security	A.5.1	Policies for information security

Licensed Under Creative Commons Attribution CC BY

		policies & programs.						

Licensed Under Creative Commons Attribution CC BY