Five Perspectives to help you understand the New PCI DSS v4.0 Requirements

Toshiro Yanagihara
Product Manager(P2PE/3DS), APAC PCI Scheme Manager
BSI Group Japan K.K.

About Us

Toshiro Yanagihara

<PCI Security Standard Qualification>
- Qualified Security Assessor(QSA)
- P2PE Assessor - 3DS Assessor

<Roles & Responsibilities at BSI Group Japan>
- Product Manager(P2PE/3DS)
- APAC PCI Scheme Manager

<Biography>
- Over 20 years of IT & Security auditing and advisory work experience with audit firm, financial institution, Japanese government and BSI Japan.
- Over 8 years of work experience of PCI related assessments and QA review
- Over 3 years of watching the trend of v4.0 development

BSI Group Japan K.K.

<PCI Security Standard Qualification>
- Qualified Security Assessor Company
- P2PE/3DS Assessor Company
- PCI Forensic Investigator Company

<Serving Markets>
- QSA, 3DS Assessor: Asia Pacific, CEMEA, LAC, Europe
- P2PE Assessor: Asia Pacific
- PCI Forensic Investigator: Japan Only

<Biography>
- Over 15 years of work experience in PCI DSS assessment in Japan and APAC.
- One of the most experienced and knowledgeable QSAC in Japan and APAC.

PCI Security Standards Council

Goals for PCI DSS v4.0

Continue to Meet the Security Needs of the Payment Industry

Promote Security as Continuous Process

Add Flexibility for Different Methodologies

Enhance Validation Methods

Quotes from "First Look at PCI DSS v4.0"

PCI Security Standards Council

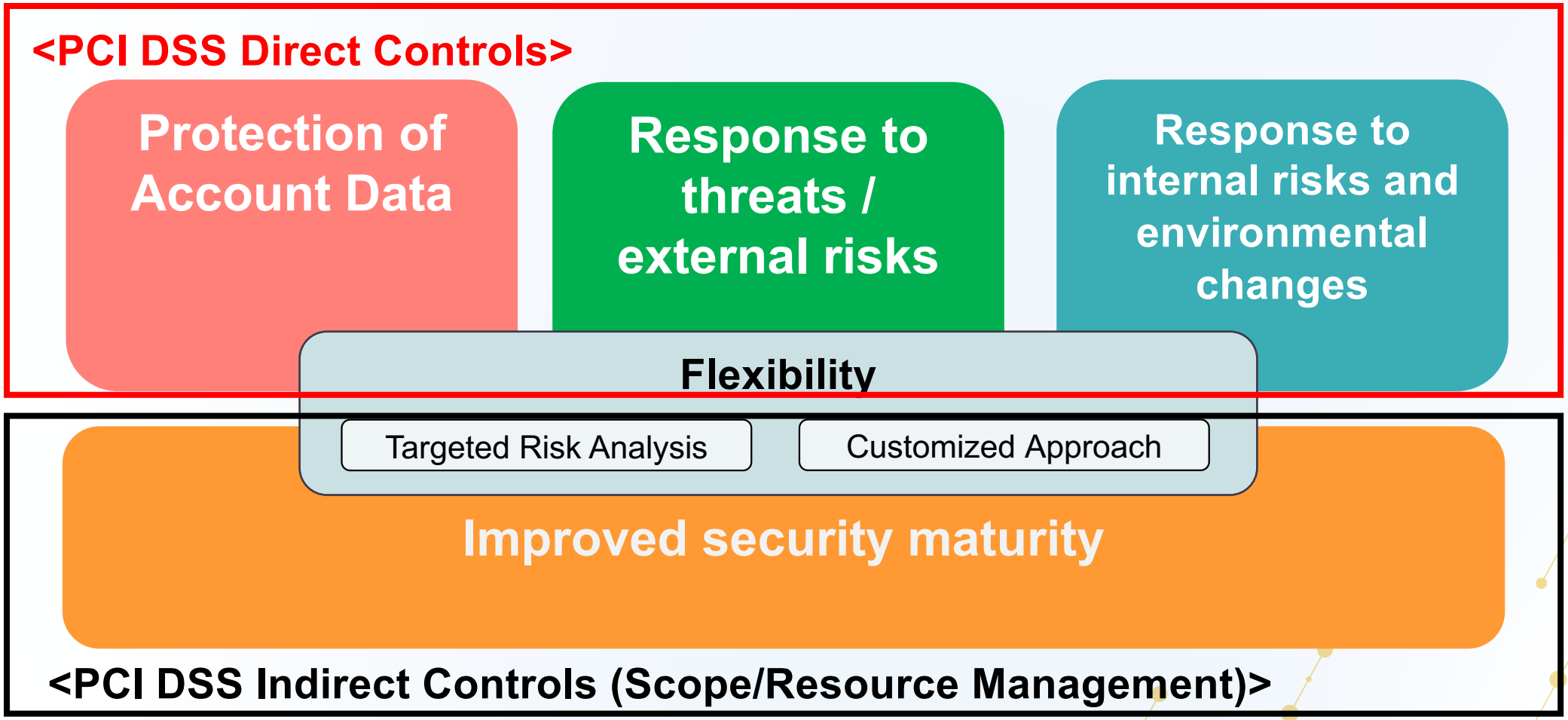
Number of New Requirements per Principal Requirement in v4.0

1	Install and Maintain Network Security Controls.	0
2	Apply Secure Configurations to All System Components.	1
3	Protect Stored Account Data.	8
4	Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks.	3
5	Protect All Systems and Networks from Malicious Software.	5
6	Develop and Maintain Secure Systems and Software.	4
7	Restrict Access to System Components and Cardholder Data by Business Need to Know.	4
8	Identify and authenticate access to system components.	8
9	Restrict Physical Access to Cardholder Data.	2
10	Log and Monitor All Access to System Components and Cardholder Data.	5
11	Test Security of Systems and Networks Regularly.	6
12	Support Information Security with Organizational Policies and Programs.	14
	Sub total (A1 – A3)	4
	Total (A1 - A3 included)	**64**

Five Perspectives

PCI Security Standards Council

Two Layers inherent in Five Perspectives



PCI Security Standards Council

What is “Protection of Account Data” ?

- “Protection of Account Data” includes nine requirements that require controls to directly protect Account Data including PAN (Primary Account Number), SAD (Sensitive Authentication data) during storing or transmission or deletion, basically using strong cryptography.

- The new requirements included in this perspective have aspects that require the installation of new processes or new technology, so the effective date for all requirements has been set as 31 March 2025.

<Important Keywords>

Protection of SAD, Protection of PAN, Protection of Account Data

PCI Security Standards Council

Protection of Account Data

	New Requirement	Apply to
3.3.2	SAD stored electronically prior to completion of authorization is encrypted using strong cryptography.	All
3.5.1.2	Implementation of disk-level or partition-level encryption when used to render PAN unreadable.	All
4.2.1	Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked.	All

Protection of Account Data

	New Requirement	Apply to
3.3.2	SAD stored electronically prior to completion of authorization is encrypted using strong cryptography.	All
3.5.1.2	Implementation of disk-level or partition-level encryption when used to render PAN unreadable.	All
4.2.1	Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked.	All

What is “Response to threats/external risks”?

- “Response to threats/external risks” includes ten requirements that require controls to detect and prevent malware or external attacks as well as conducting periodic controls based on the results of Targeted Risk Analysis.
- The new requirements included in this perspective have aspects that require the installation of new processes or new technology, so the effective date for all requirements has been set as 31 March 2025.

<Important Keywords>

Phishing attacks, Web-based attacks, Skimming attacks, Response to malware
Payment page tampering, Covert malware communication channels, POI device inspections

PCI Security Standards Council

Response to External Threats/Risks

	New Requirement	Apply to
5.4.1	Mechanisms are in place to detect and protect personnel against phishing attacks.	All
6.4.3	Manage all payment page scripts that are loaded and executed in the consumer's browser.	All
11.6.1	A change-and-tamper-detection mechanism is deployed for payment pages.	All
12.6.3.1	Security awareness training includes awareness of threats that could impact the security of the CDE, to include phishing and related attacks and social engineering.	All

Response to External Threats/Risks

	New Requirement	Apply to
5.4.1	Mechanisms are in place to detect and protect personnel against phishing attacks.	All
6.4.3	Manage all payment page scripts that are loaded and executed in the consumer's browser.	All
11.6.1	A change-and-tamper-detection mechanism is deployed for payment pages.	All
12.6.3.1	Security awareness training includes awareness of threats that could impact the security of the CDE, to include phishing and related attacks and social engineering.	All

What is “Response to Internal Risks and Environmental Changes ”?

- “Response to Internal Risks and Environmental Changes” includes twenty three requirements that require to strengthen existing controls regarding Password, MFA (Multi-Factor Authentication) and Authenticated scan as well as to add new controls for Account Management regarding application and system accounts.

- The new requirements included in this perspective have aspects that require the installation of new processes or new technology, so the effective date for all requirements has been set as 31 March 2025 except requirement 12.9.2.

<Important Keywords>

Account Management, Password, MFA (Multi-Factor Authentication) , Response to Vulnerability
Authenticated Scan, Audit log reviews, Critical security control systems
Customer support by TPSP (Third Party Service Provider) , Multi-tenant service provider

PCI Security Standards Council

What is “Response to Internal Risks and Environmental Changes ”?

- “Response to Internal Risks and Environmental Changes” includes twenty three requirements that require to strengthen existing controls regarding Password, MFA (Multi-Factor Authentication) and Authenticated scan as well as to add new controls for Account Management regarding application and system accounts.

- The new requirements included in this perspective have aspects that require the installation of new processes or new technology, so the effective date for all requirements has been set as 31 March 2025 except requirement 12.9.2.

<Important Keywords>

Account Management, Password, MFA (Multi-Factor Authentication) , Response to Vulnerability
Authenticated Scan, Audit log reviews, Critical security control systems
Customer support by TPSP (Third Party Service Provider) , Multi-tenant service provider

PCI Security Standards Council

Response to Internal Risks and Environmental Changes

	New Requirement	Apply to
7.2.4	Review all user accounts and related access privileges appropriately.	All
8.3.6	Minimum level of complexity for passwords when used as an authentication factor.	All
8.4.2	Multi-factor authentication for all access into the CDE.	All
8.5.1	Multi-factor authentication systems are implemented appropriately.	All
10.4.1.1	Audit log reviews are automated.	All
11.3.1.2	Internal vulnerability scans are performed via authenticated scanning.	All

Response to Internal Risks and Environmental Changes

	New Requirement	Apply to
7.2.4	Review all user accounts and related access privileges appropriately.	All
8.3.6	Minimum level of complexity for passwords when used as an authentication factor.	All
8.4.2	Multi-factor authentication for all access into the CDE.	All
8.5.1	Multi-factor authentication systems are implemented appropriately.	All
10.4.1.1	Audit log reviews are automated.	All
11.3.1.2	Internal vulnerability scans are performed via authenticated scanning.	All

Response to Internal Risks and Environmental Changes

	New Requirement	Apply to
7.2.4	Review all user accounts and related access privileges appropriately.	All
8.3.6	Minimum level of complexity for passwords when used as an authentication factor.	All
8.4.2	Multi-factor authentication for all access into the CDE.	All
8.5.1	Multi-factor authentication systems are implemented appropriately.	All
10.4.1.1	Audit log reviews are automated.	All
11.3.1.2	Internal vulnerability scans are performed via authenticated scanning.	All

What is “Flexibility”?

- “Flexibility” includes two requirements that require to conduct Targeted Risk Analysis for “Periodic Controls” and “Customized Controls”.
- The aim of “Flexibility” is that the entity can determine necessary controls against applicable requirements in accordance with their will and risk environment.
- The new requirement 12.3.1 for “Periodic Controls” included in this perspective have aspects that require the installation of new processes or new technology, so the effective date has been set as 31 March 2025. However, the effective date of the requirement 12.3.2 for “Customized Controls” has been set as immediately.

<Important Keywords>

Customized Approach, Targeted Risk Analysis

PCI Security Standards Council

Flexibility

	New Requirement	Apply to
12.3.1	A targeted risk analysis is documented to support each PCI DSS requirement that provides flexibility for how frequently it is performed.	All
12.3.2	A targeted risk analysis is performed for each PCI DSS requirement that is met with the customized approach.	All

Flexibility

	New Requirement	Apply to
12.3.1	A targeted risk analysis is documented to support each PCI DSS requirement that provides flexibility for how frequently it is performed.	All
12.3.2	A targeted risk analysis is performed for each PCI DSS requirement that is met with the customized approach.	All

Flexibility (Periodic Controls)

	New Requirement	Apply to
5.2.3.1	A targeted risk analysis is performed to determine frequency of periodic evaluations of system components identified as not at risk for malware.	All
5.3.2.1	A targeted risk analysis is performed to determine frequency of periodic malware scans.	All
7.2.5.1	Review all access by application and system accounts and related access privileges.	All
8.6.3	Passwords/passphrases for any application and system accounts are protected against misuse.	All
9.5.1.2.1	A targeted risk analysis is performed to determine frequency of periodic POI device inspections.	All
10.4.2.1	A targeted risk analysis is performed to determine frequency of log reviews for all other system components.	All
11.3.1.1	Manage all other applicable vulnerabilities (those not ranked as high-risk or critical).	All
11.6.1	A change-and-tamper-detection mechanism is deployed for payment pages.	All
12.10.4.1	A targeted risk analysis is performed to determine frequency of periodic training for incident response personnel.	All

Flexibility (Periodic Controls)

	New Requirement	Apply to
5.2.3.1	A targeted risk analysis is performed to determine frequency of periodic evaluations of system components identified as not at risk for malware.	All
5.3.2.1	A targeted risk analysis is performed to determine frequency of periodic malware scans.	All
7.2.5.1	Review all access by application and system accounts and related access privileges.	All
8.6.3	Passwords/passphrases for any application and system accounts are protected against misuse.	All
9.5.1.2.1	A targeted risk analysis is performed to determine frequency of periodic POI device inspections.	All
10.4.2.1	A targeted risk analysis is performed to determine frequency of log reviews for all other system components.	All
11.3.1.1	Manage all other applicable vulnerabilities (those not ranked as high-risk or critical).	All
11.6.1	A change-and-tamper-detection mechanism is deployed for payment pages.	All
12.10.4.1	A targeted risk analysis is performed to determine frequency of periodic training for incident response personnel.	All

What is “Improved Security Maturity”?

- “Improved Security Maturity” includes twenty requirements that consist of eleven requirements applied immediately and nine requirements applied after 31 March 2025.
- The requirements included in this perspective aim to install PCI DSS indirect controls that are targeted to PCI DSS scope/resources for supporting PCI DSS direct controls. For example, Site, Location, People, Organization, Knowledge, Process, Technology and Flexible Controls.
- We can understand that the requirements in “Improved Security Maturity” and “Flexibility” are PCI DSS indirect controls and completely different from other perspectives that are classified as PCI DSS direct controls including “Protection of Account Data”, “Response to threats / external risks”, “Response to internal risks and environmental changes”.

<Important Keywords>
Roles & Responsibility, Annual PCI DSS Scope Confirmation, Resource Review, Security awareness program, Security incident response plan

PCI Security Standards Council

Improved Security Maturity

	New Requirement	Apply to
2.1.2 to 11.1.2	Roles and responsibilities for performing activities in Requirement 2 to 11 are documented, assigned, and understood.	All
12.3.3	Cryptographic cipher suites and protocols in use are documented and reviewed.	All
12.3.4	Hardware and software technologies are reviewed.	All
12.5.2	PCI DSS scope is documented and confirmed at least once every 12 months.	All
12.6.2	The security awareness program is reviewed at least once every 12 months and updated as needed.	All
12.10.5	The security incident response plan includes alerts from the change- and tamper-detection mechanism for payment pages.	All
12.10.7	Incident response procedures are in place and initiated upon detection of PAN.	All

Improved Security Maturity

	New Requirement	Apply to
2.1.2 to 11.1.2	Roles and responsibilities for performing activities in Requirement 2 to 11 are documented, assigned, and understood.	All
12.3.3	Cryptographic cipher suites and protocols in use are documented and reviewed.	All
12.3.4	Hardware and software technologies are reviewed.	All
12.5.2	PCI DSS scope is documented and confirmed at least once every 12 months.	All
12.6.2	The security awareness program is reviewed at least once every 12 months and updated as needed.	All
12.10.5	The security incident response plan includes alerts from the change- and tamper-detection mechanism for payment pages.	All
12.10.7	Incident response procedures are in place and initiated upon detection of PAN.	All

Improved Security Maturity

	New Requirement	Apply to
2.1.2 to 11.1.2	Roles and responsibilities for performing activities in Requirement 2 to 11 are documented, assigned, and understood.	All
12.3.3	Cryptographic cipher suites and protocols in use are documented and reviewed.	All
12.3.4	Hardware and software technologies are reviewed.	All
12.5.2	PCI DSS scope is documented and confirmed at least once every 12 months.	All
12.6.2	The security awareness program is reviewed at least once every 12 months and updated as needed.	All
12.10.5	The security incident response plan includes alerts from the change- and tamper-detection mechanism for payment pages.	All
12.10.7	Incident response procedures are in place and initiated upon detection of PAN.	All

Two considerations for v4.0 initial assessment before 31 March 2025

1	**Dealing with Introduction Section changes in v4.0 - Items that may affect multiple requirements** ● Expansion of the definition of Cardholder Data Environment (CDE) ● Requirements that the target was changed from cardholder data (CHD) to Account Data ● New time frame guidelines have been established, for example, as follows; - Every 3 months: At least once every 90 to 92 days, or on the nth day of each third month. - Every 6 months: At least once every 180 to 184 days, or on the nth day of each sixth month. - Significant Change: Any changes that have potential impact on the security of the CDE.
2	**Responding to new requirements that will be applied immediately (13 requirements)** ● Roles and Responsibilities: requirement 2.1.2 to 11.1.2, 10 requirements in total ● Annual PCI DSS Scope Confirmation: requirement 12.5.2, All Entities ● Customer support by Third Party Service Provider: requirement 12.9.2, Service Provider Only ● Targeted Risk Analysis for Customized Approach: requirement 12.3.2, when applicable

PCI Security Standards Council

Two considerations for v4.0 initial assessment before 31 March 2025

1	**Dealing with Introduction Section changes in v4.0 - Items that may affect multiple requirements** ● Expansion of the definition of Cardholder Data Environment (CDE) ● Requirements that the target was changed from cardholder data (CHD) to Account Data ● New time frame guidelines have been established, for example, as follows; - Every 3 months: At least once every 90 to 92 days, or on the nth day of each third month. - Every 6 months: At least once every 180 to 184 days, or on the nth day of each sixth month. - Significant Change: Any changes that have potential impact on the security of the CDE.
2	**Responding to new requirements that will be applied immediately (13 requirements)** ● Roles and Responsibilities: requirement 2.1.2 to 11.1.2, 10 requirements in total ● Annual PCI DSS Scope Confirmation: requirement 12.5.2, All Entities ● Customer support by Third Party Service Provider: requirement 12.9.2, Service Provider Only ● Targeted Risk Analysis for Customized Approach: requirement 12.3.2, when applicable

PCI Security Standards Council

Supplemental Information on Introduction Section Changes

Expansion of the definition of Cardholder Data Environment (CDE)

- The following underlined part was added.
  "The cardholder data environment (CDE), which is comprised of:
  – System components, people, and processes that store, process, and transmit cardholder data and/or sensitive authentication data, and,
  – System components that may not store, process, or transmit CHD/SAD but have unrestricted connectivity to system components that store, process, or transmit CHD/SAD."
- For example, added system components to CDE may include authentication servers, remote access servers, logging servers etc.
- It is required to consider the impact of the CDE definition change in Annual PCI DSS Scope Confirmation.

Requirements that the target was changed from cardholder data (CHD) to Account Data

- Additional investigation of the impact to scope may be necessary along with Annual PCI DSS Scope Confirmation.
- For example,
  - requirement 1.2.4: Account Data Flow-Diagram
  - requirement 3.2.1: Account data storage etc.

PCI Security Standards Council

Supplemental Information on Introduction Section Changes

Expansion of the definition of Cardholder Data Environment (CDE)

- The following underlined part was added.
  "The cardholder data environment (CDE), which is comprised of:
  – System components, people, and processes that store, process, and transmit cardholder data and/or sensitive authentication data, and,
  – System components that may not store, process, or transmit CHD/SAD but have unrestricted connectivity to system components that store, process, or transmit CHD/SAD."
- For example, added system components to CDE may include authentication servers, remote access servers, logging servers etc.
- It is required to consider the impact of the CDE definition change in Annual PCI DSS Scope Confirmation.

Requirements that the target was changed from cardholder data (CHD) to Account Data

- Additional investigation of the impact to scope may be necessary along with Annual PCI DSS Scope Confirmation.
- For example,
  - requirement 1.2.4: Account Data Flow-Diagram
  - requirement 3.2.1: Account data storage etc.

PCI Security Standards Council

Two considerations toward v4.0 assessment after 31 March 2025

1	**Responding to New requirements that require consideration of installation of Automated Controls** • Of the 51 requirements that would become effective after 31 March 2025, I assume there are 25 requirements that are expected to require automated solutions and are recommended to be considered for implementation. • These new requirements require time and cost to research, select, procure, and implement solutions, so it is recommended to prepare a plan and start with what is possible.
2	**Responding to New requirements that require consideration of installation of Manual Controls** • I assume there are 26 new requirements that need to be addressed using manual controls. • These new requirements include some complex and time-consuming elements that were not there before, so it is recommended to prepare a plan and start with what is possible.

PCI Security Standards Council