2025
ASIA-PACIFIC
COMMUNITY
MEETING

Blueprint for the Future

Modernizing PCI SSC Standards and Supporting Documentation

PCI Security Standards Council®

Jake Marcinko

Senior Technical Product Manager

PCI Security Standards Council

PCI Security Standards Council®

Session Agenda

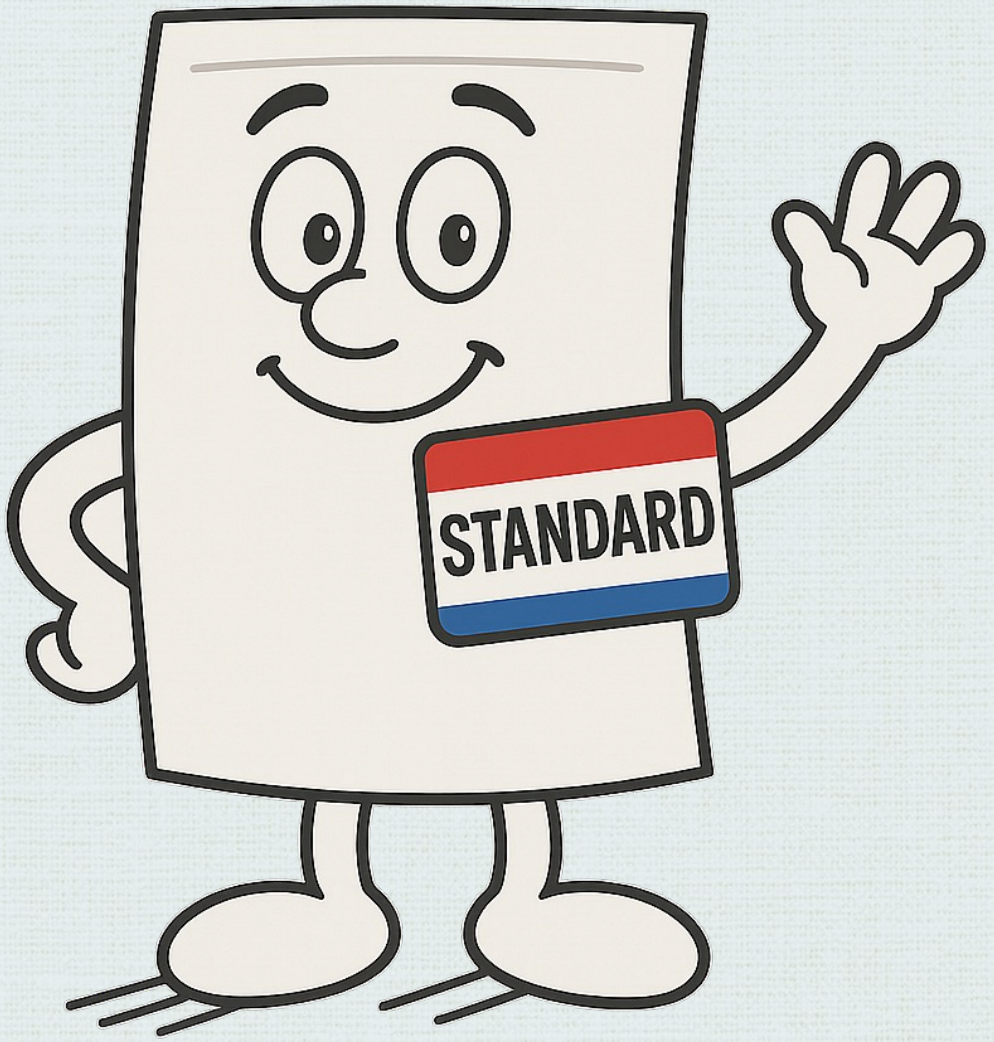
What is the Standards Modernization initiative?

Why is it important?

What is it intended to achieve?

PCI Security Standards Council

PCI Security Standards Council

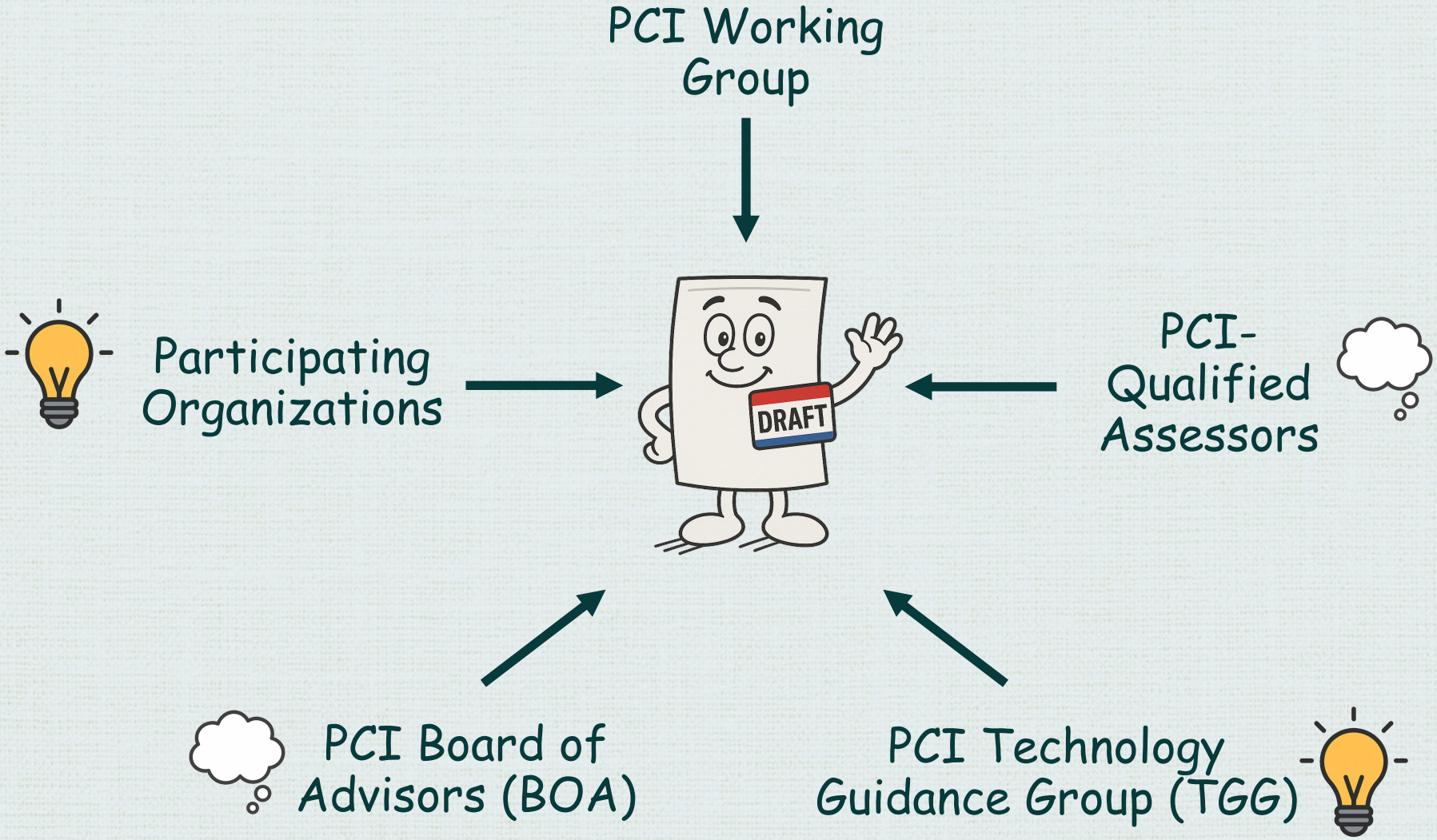


PCI Security Standards Council

Standards Development Process

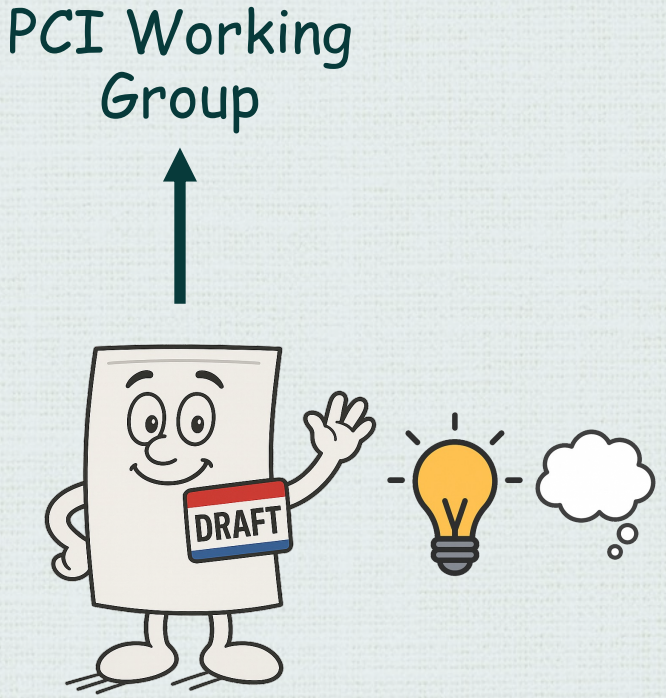
PCI Working Group

Standards Development Process

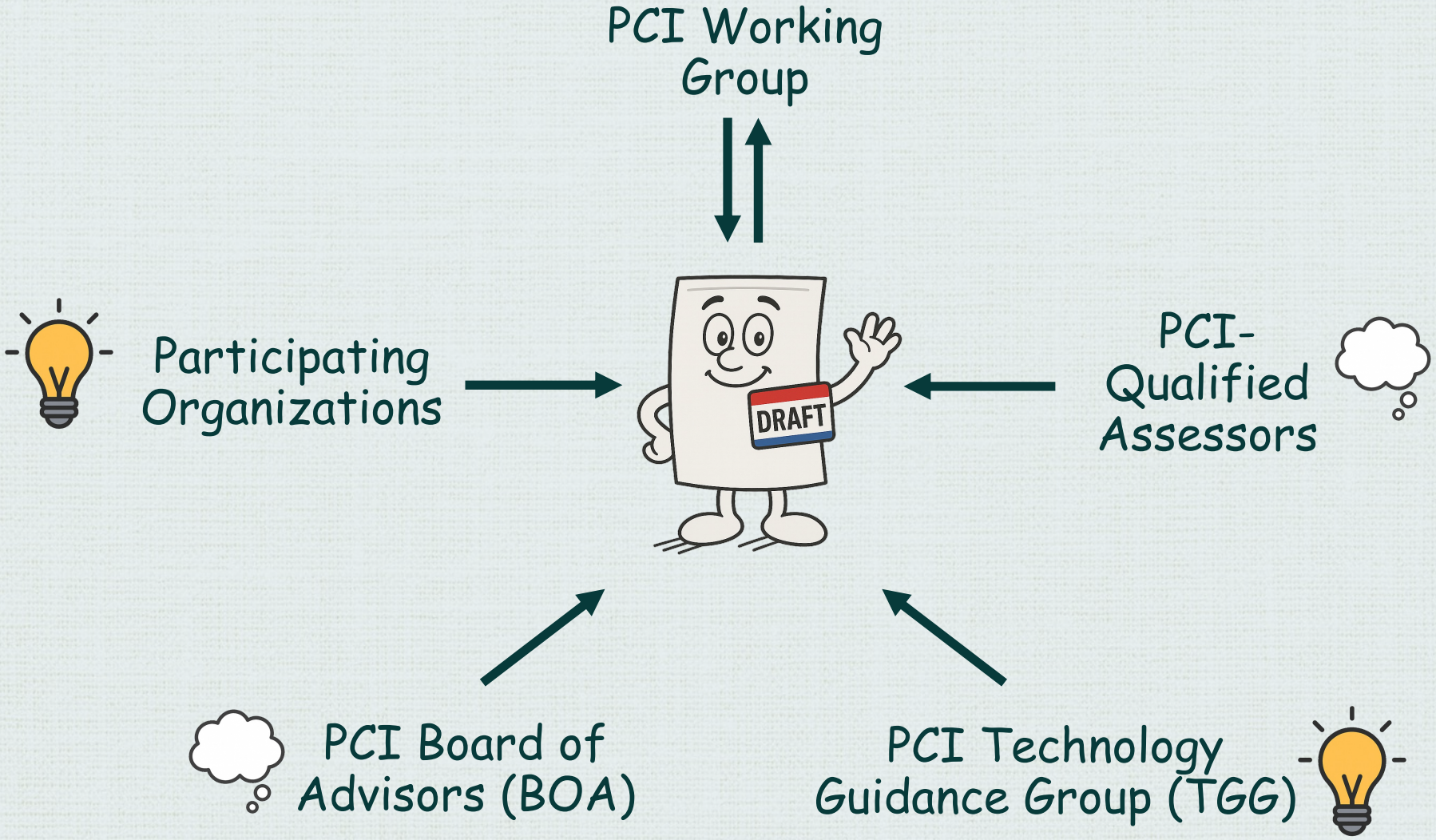


PCI Security Standards Council

Standards Development Process



Standards Development Process



PCI Security Standards Council

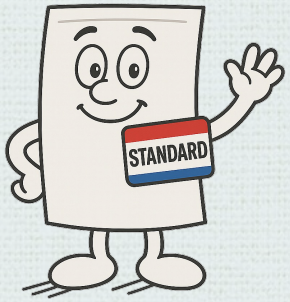
Internal Approvals

Working Group

→

Internal PCI Stakeholder Reviews & Approvals

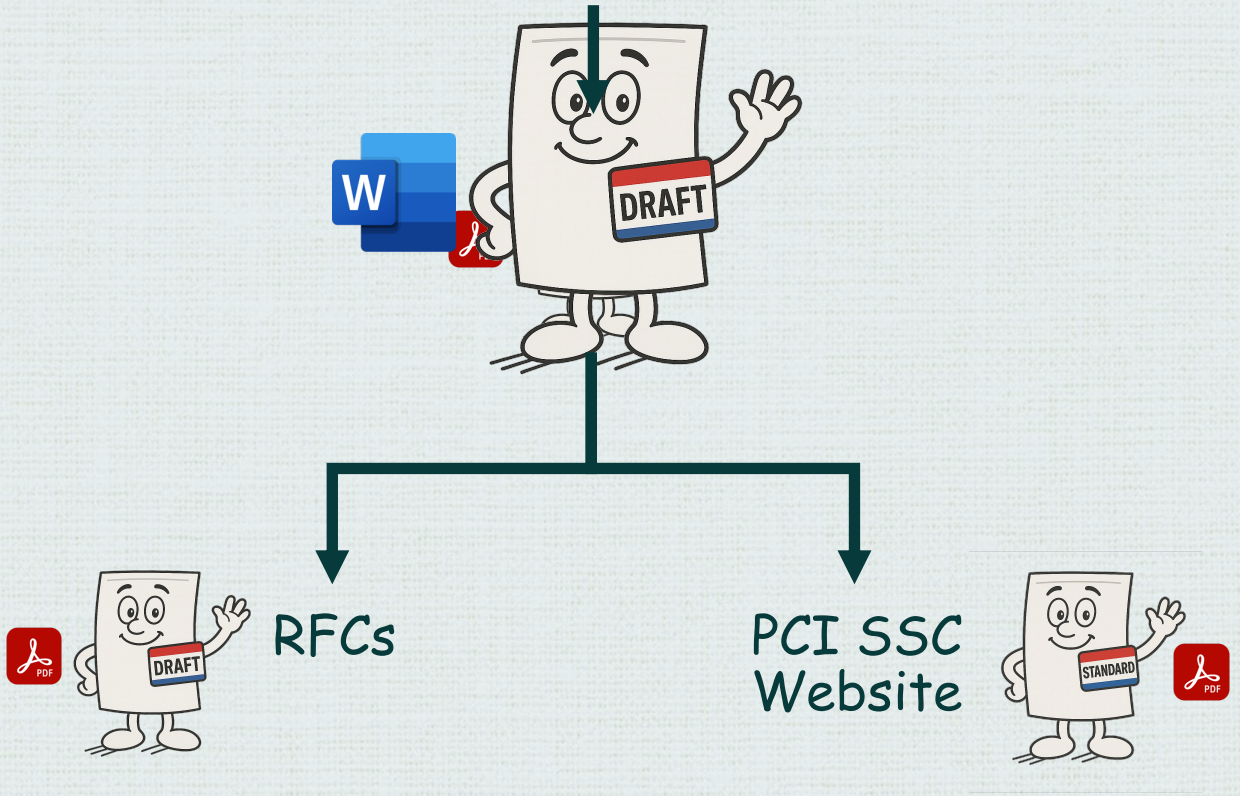
→



Publication

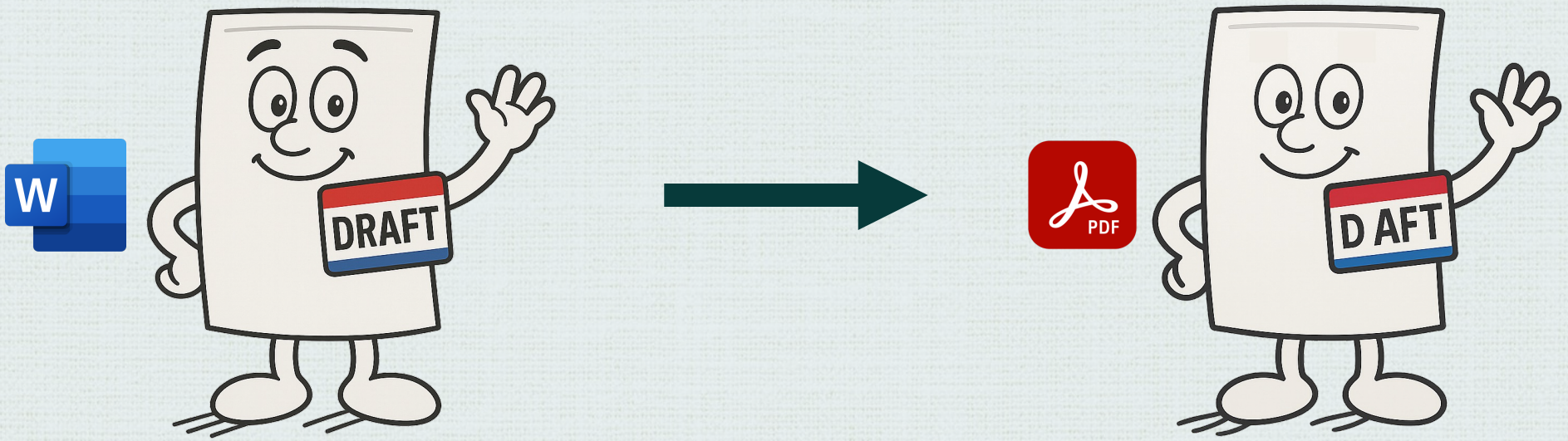
PCI Security Standards Council

Document Creation and Conversion



Challenge #1: Data Loss

Challenge #1: Data Loss



Challenge #2: Usability

Challenge #2: Usability

PCI Security Standards Council

15 Detailed PCI DSS Requirements and Testing Procedures

Figure 5 describes the column headings and content for the PCI DSS requirements.

Figure 5. Understanding the Parts of the Requirements

The **Requirement Description** at the X.X level organizes and describes the requirements that fall under it.

The **Defined Approach Requirements and Testing Procedures** describes the traditional method for implementing and validating PCI DSS using the Requirements and Testing Procedures defined in the standard.

The **Customized Approach Objective** is the intended goal or outcome for the requirement. It must be met by entities using a Customized Approach. Most PCI DSS requirements have this Objective.

Appendix D describes expectations for entities and assessors when the Customized Approach is used.

Entities following the Defined Approach can refer to the **Customized Approach Objective** as guidance, but the objective does not replace or supersede the Defined Approach Requirement.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
3.4.2 When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need.	**3.4.2.a** Examine documented policies and procedures and documented evidence for technical controls that prevent copy and/or relocation of PAN when using remote-access technologies onto local hard drives or removable electronic media to verify the following: • Technical controls prevent all personnel not specifically authorized from copying and/or relocating PAN. • A list of personnel with permission to copy and/or relocate PAN is maintained, together with the documented, explicit authorization and legitimate, defined business need.	Relocation of PAN to unauthorized storage devices is a common way for this data to be obtained and used fraudulently. Methods to ensure that only those with explicit authorization and a legitimate business reason can copy or relocate PAN minimizes the risk of unauthorized persons gaining access to PAN.
Customized Approach Objective		**Good Practice**
PAN cannot be copied or relocated by unauthorized personnel using remote-access technologies.		Copying and relocation of PAN should only be done to storage devices that are permissible and authorized for that individual.
Applicability Notes	**3.4.2.b** Examine configurations for remote-access technologies to verify that technical controls to prevent copy and/or relocation of PAN for all personnel, unless explicitly authorized.	**Definitions**
Storing or relocating PAN onto local hard drives, removable electronic media, and other storage devices brings these devices into scope for PCI DSS. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	**3.4.2.c** Observe processes and interview personnel to verify that only personnel with documented, explicit authorization and a legitimate, defined business need have permission to copy and/or relocate PAN when using remote-access technologies.	A virtual desktop is an example of a remote-access technology. Storage devices include, but are not limited to, local hard drives, virtual drives, removable electronic media, network drives, and cloud storage.
		Examples
		Further Information Vendor documentation for the remote-access technology in use will provide information about the system settings needed to implement this requirement.

Applicability Notes apply to both the Defined and Customized Approach. It includes information that affects how the requirement is interpreted in the context of the entity or in scoping.

These notes are an integral part of PCI DSS and must be fully considered during an assessment.

For each new PCI DSS v4.x requirement with an extended implementation period.

Guidance provides information to understand how to meet a requirement. Guidance is not required to be followed – it does not replace or extend any PCI DSS requirement.

Not every **Guidance** section described here is present for each requirement.

Not every section will be present for each requirement.

Purpose describes the goal, benefit, or threat to be avoided; why the requirement exists.

A **Good Practice** can be considered by the entity when meeting a requirement.

Definitions Terms that may help understand the requirement.

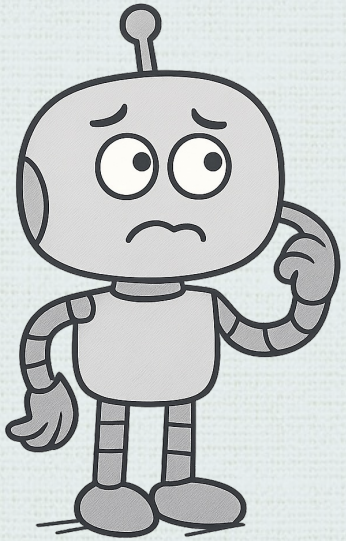
Examples describe ways a requirement could be met.

Further Information includes references to relevant external documentation.

PCI Security Standards Council

Challenge #2: Usability

Machine Interpretability



PCI Security Standards Council

15 Detailed PCI DSS Requirements and Testing Procedures

Figure 5 describes the column headings and content for the PCI DSS requirements.

Figure 5. Understanding the Parts of the Requirements

The **Requirement Description** at the X.X level organizes and describes the requirements that fall under it.

The **Defined Approach Requirements and Testing Procedures** describes the traditional method for implementing and validating PCI DSS using the Requirements and Testing Procedures defined in the standard.

The **Customized Approach Objective** is the intended goal or outcome for the requirement. It must be met by entities using a Customized Approach. Most PCI DSS requirements have this Objective.

Appendix D describes expectations for entities and assessors when the Customized Approach is used.

Entities following the Defined Approach can refer to the **Customized Approach Objective** as guidance, but the objective does not replace or supersede the Defined Approach Requirement.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
3.4.2 When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need.	**3.4.2.a** Examine documented policies and procedures and documented evidence for technical controls that prevent copy and/or relocation of PAN when using remote-access technologies onto local hard drives or removable electronic media to verify the following: • Technical controls prevent all personnel not specifically authorized from copying and/or relocating PAN. • A list of personnel with permission to copy and/or relocate PAN is maintained, together with the documented, explicit authorization and legitimate, defined business need.	Relocation of PAN to unauthorized storage devices is a common way for this data to be obtained and used fraudulently. Methods to ensure that only those with explicit authorization and a legitimate business reason can copy or relocate PAN minimizes the risk of unauthorized persons gaining access to PAN. **Good Practice** Copying and relocation of PAN should only be done to storage devices that are permissible and authorized for that individual. **Definitions** A virtual desktop is an example of a remote-access technology. Storage devices include, but are not limited to, local hard drives, virtual drives, removable electronic media, network drives, and cloud storage. **Examples** **Further Information** Vendor documentation for the remote-access technology in use will provide information about the system settings needed to implement this requirement.
Customized Approach Objective		
PAN cannot be copied or relocated by unauthorized personnel using remote-access technologies.		
Applicability Notes	**3.4.2.b** Examine configurations for remote-access technologies to verify that technical controls to prevent copy and/or relocation of PAN for all personnel, unless explicitly authorized.	
Storing or relocating PAN onto local hard drives, removable electronic media, and other storage devices brings these devices into scope for PCI DSS. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	**3.4.2.c** Observe processes and interview personnel to verify that only personnel with documented, explicit authorization and a legitimate, defined business need have permission to copy and/or relocate PAN when using remote-access technologies.	

Applicability Notes apply to both the Defined and Customized Approach. It includes information that affects how the requirement is interpreted in the context of the entity or in scoping.

These notes are an integral part of PCI DSS and must be fully considered during an assessment.

For each new PCI DSS v4.x requirement with an extended implementation period.

Guidance provides information to understand how to meet a requirement. Guidance is not required to be followed – it does not replace or extend any PCI DSS requirement.

Not every **Guidance** section described here is present for each requirement.

Not every section will be present for each requirement.

Purpose describes the goal, benefit, or threat to be avoided; why the requirement exists.

A **Good Practice** can be considered by the entity when meeting a requirement.

Definitions Terms that may help understand the requirement.

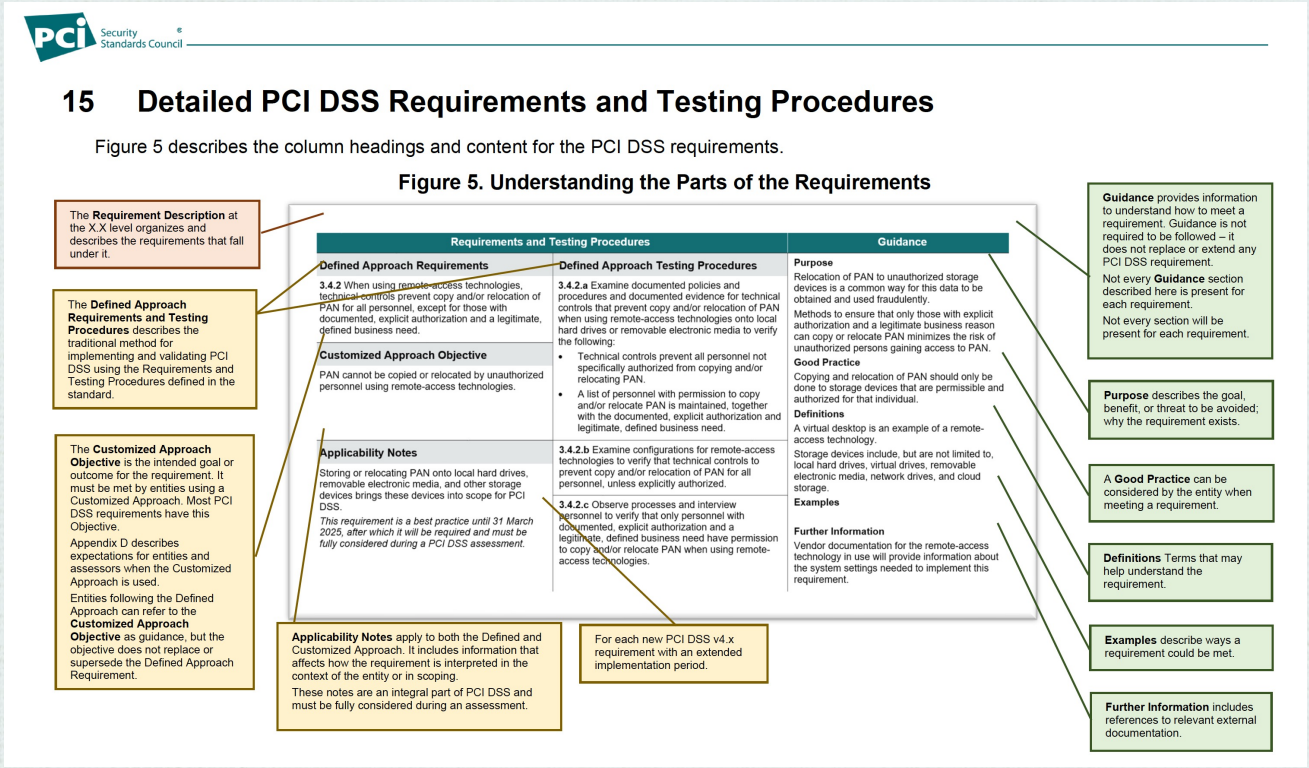
Examples describe ways a requirement could be met.

Further Information includes references to relevant external documentation.

PCI Security Standards Council

Challenge #2: Usability

Accessibility



PCI Security Standards Council

15 Detailed PCI DSS Requirements and Testing Procedures

Figure 5 describes the column headings and content for the PCI DSS requirements.

Figure 5. Understanding the Parts of the Requirements

The **Requirement Description** at the X.X level organizes and describes the requirements that fall under it.

The **Defined Approach Requirements and Testing Procedures** describes the traditional method for implementing and validating PCI DSS using the Requirements and Testing Procedures defined in the standard.

The **Customized Approach Objective** is the intended goal or outcome for the requirement. It must be met by entities using a Customized Approach. Most PCI DSS requirements have this Objective.

Appendix D describes expectations for entities and assessors when the Customized Approach is used.

Entities following the Defined Approach can refer to the **Customized Approach Objective** as guidance, but the objective does not replace or supersede the Defined Approach Requirement.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Relocation of PAN to unauthorized storage devices is a common way for this data to be obtained and used fraudulently. Methods to ensure that only those with explicit authorization and a legitimate business reason can copy or relocate PAN minimizes the risk of unauthorized persons gaining access to PAN. **Good Practice** Copying and relocation of PAN should only be done to storage devices that are permissible and authorized for that individual. **Definitions** A virtual desktop is an example of a remote-access technology. Storage devices include, but are not limited to, local hard drives, virtual drives, removable electronic media, network drives, and cloud storage. **Examples** **Further Information** Vendor documentation for the remote-access technology in use will provide information about the system settings needed to implement this requirement.
3.4.2 When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need.	**3.4.2.a** Examine documented policies and procedures and documented evidence for technical controls that prevent copy and/or relocation of PAN when using remote-access technologies onto local hard drives or removable electronic media to verify the following: • Technical controls prevent all personnel not specifically authorized from copying and/or relocating PAN. • A list of personnel with permission to copy and/or relocate PAN is maintained, together with the documented, explicit authorization and legitimate, defined business need.	
Customized Approach Objective PAN cannot be copied or relocated by unauthorized personnel using remote-access technologies.		
Applicability Notes Storing or relocating PAN onto local hard drives, removable electronic media, and other storage devices brings these devices into scope for PCI DSS. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	**3.4.2.b** Examine configurations for remote-access technologies to verify that technical controls to prevent copy and/or relocation of PAN for all personnel, unless explicitly authorized. **3.4.2.c** Observe processes and interview personnel to verify that only personnel with documented, explicit authorization and a legitimate, defined business need have permission to copy and/or relocate PAN when using remote-access technologies.	

Applicability Notes apply to both the Defined and Customized Approach. It includes information that affects how the requirement is interpreted in the context of the entity or in scoping.

These notes are an integral part of PCI DSS and must be fully considered during an assessment.

For each new PCI DSS v4.x requirement with an extended implementation period.

Guidance provides information to understand how to meet a requirement. Guidance is not required to be followed – it does not replace or extend any PCI DSS requirement.

Not every **Guidance** section described here is present for each requirement.

Not every section will be present for each requirement.

Purpose describes the goal, benefit, or threat to be avoided; why the requirement exists.

A **Good Practice** can be considered by the entity when meeting a requirement.

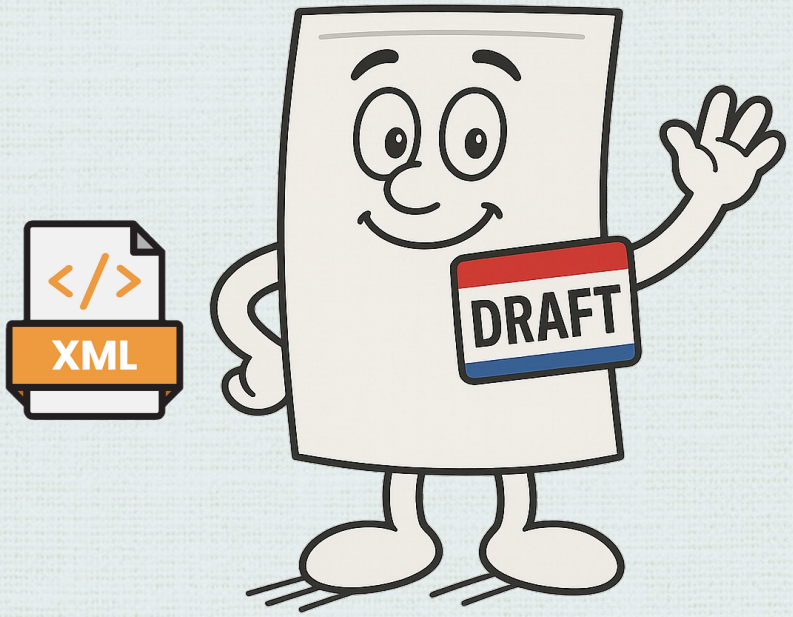
Definitions Terms that may help understand the requirement.

Examples describe ways a requirement could be met.

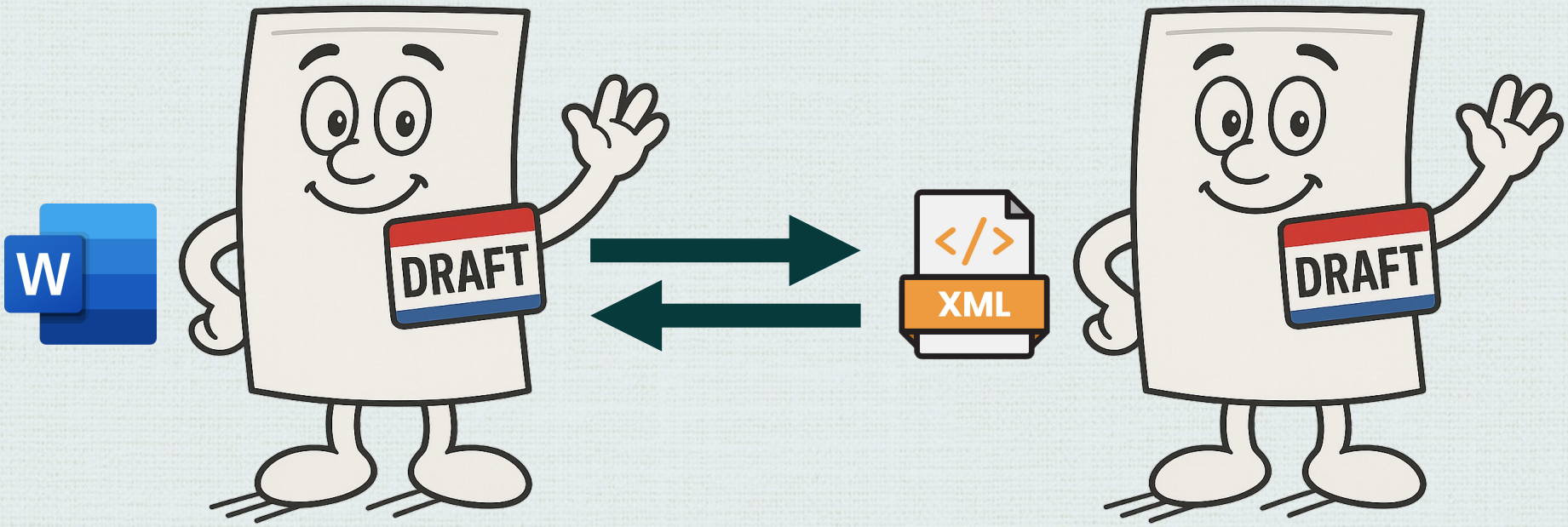
Further Information includes references to relevant external documentation.

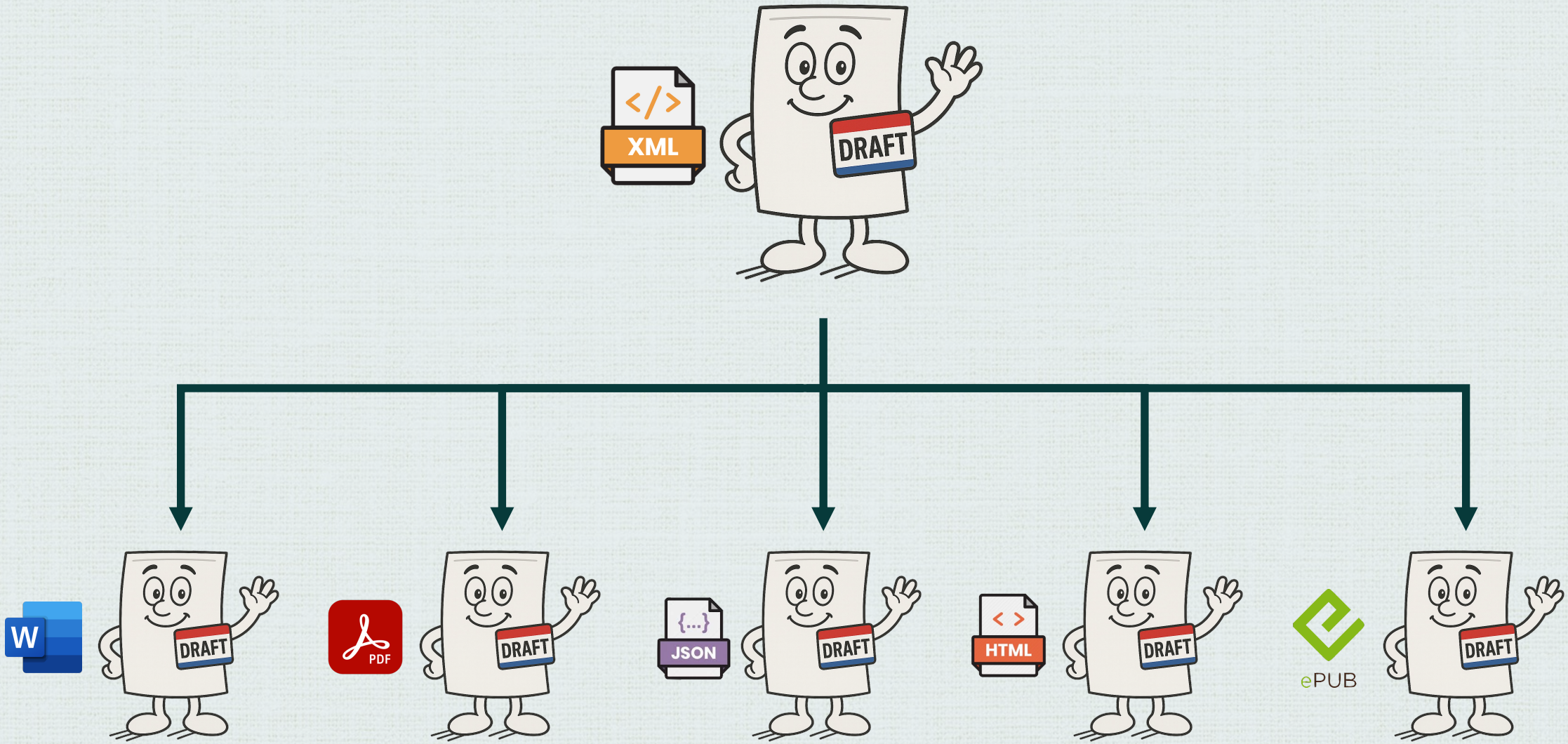
PCI Security Standards Council

The Solution?



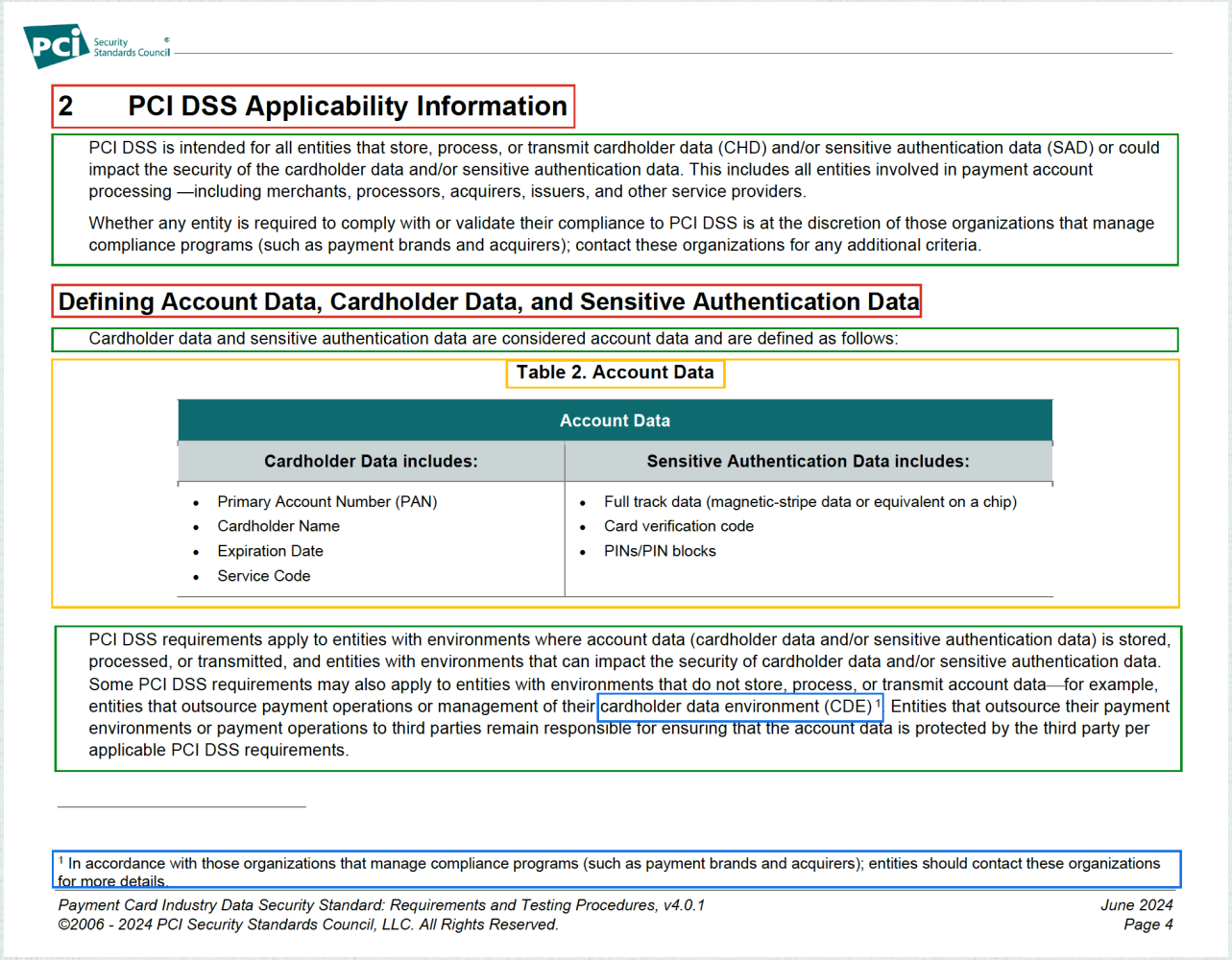
PCI Security Standards Council


W
DRAFT
</>
XML
DRAFT



PCI Security Standards Council

Content Analysis / Semantic Tagging



2 PCI DSS Applicability Information

PCI DSS is intended for all entities that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) or could impact the security of the cardholder data and/or sensitive authentication data. This includes all entities involved in payment account processing —including merchants, processors, acquirers, issuers, and other service providers.

Whether any entity is required to comply with or validate their compliance to PCI DSS is at the discretion of those organizations that manage compliance programs (such as payment brands and acquirers); contact these organizations for any additional criteria.

Defining Account Data, Cardholder Data, and Sensitive Authentication Data

Cardholder data and sensitive authentication data are considered account data and are defined as follows:

Table 2. Account Data

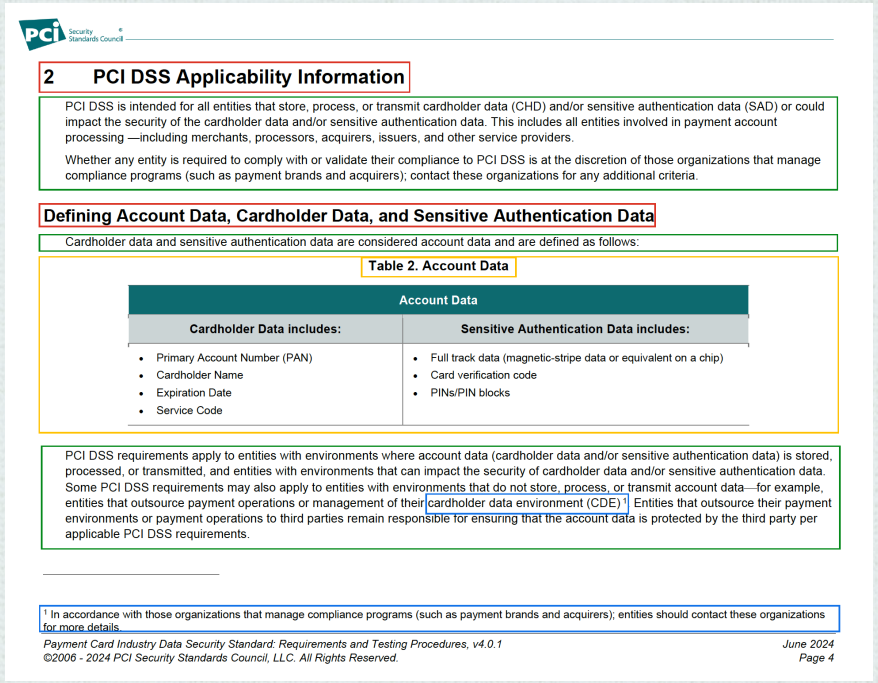
Account Data	
Cardholder Data includes:	**Sensitive Authentication Data includes:**
• Primary Account Number (PAN) • Cardholder Name • Expiration Date • Service Code	• Full track data (magnetic-stripe data or equivalent on a chip) • Card verification code • PINs/PIN blocks

PCI DSS requirements apply to entities with environments where account data (cardholder data and/or sensitive authentication data) is stored, processed, or transmitted, and entities with environments that can impact the security of cardholder data and/or sensitive authentication data. Some PCI DSS requirements may also apply to entities with environments that do not store, process, or transmit account data—for example, entities that outsource payment operations or management of their cardholder data environment (CDE) [1]. Entities that outsource their payment environments or payment operations to third parties remain responsible for ensuring that the account data is protected by the third party per applicable PCI DSS requirements.

[1] In accordance with those organizations that manage compliance programs (such as payment brands and acquirers); entities should contact these organizations for more details.

Section Heading
Paragraph Text
Table Reference
Table Title
Table Heading
Table Text
List Text
Footnote Reference
Footnote Text
Definition Reference
Figure Reference
Security Objective
Security Requirement
Test Requirement
etc.

XML Mapping



2 PCI DSS Applicability Information

PCI DSS is intended for all entities that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) or could impact the security of the cardholder data and/or sensitive authentication data. This includes all entities involved in payment account processing —including merchants, processors, acquirers, issuers, and other service providers.

Whether any entity is required to comply with or validate their compliance to PCI DSS is at the discretion of those organizations that manage compliance programs (such as payment brands and acquirers); contact these organizations for any additional criteria.

Defining Account Data, Cardholder Data, and Sensitive Authentication Data

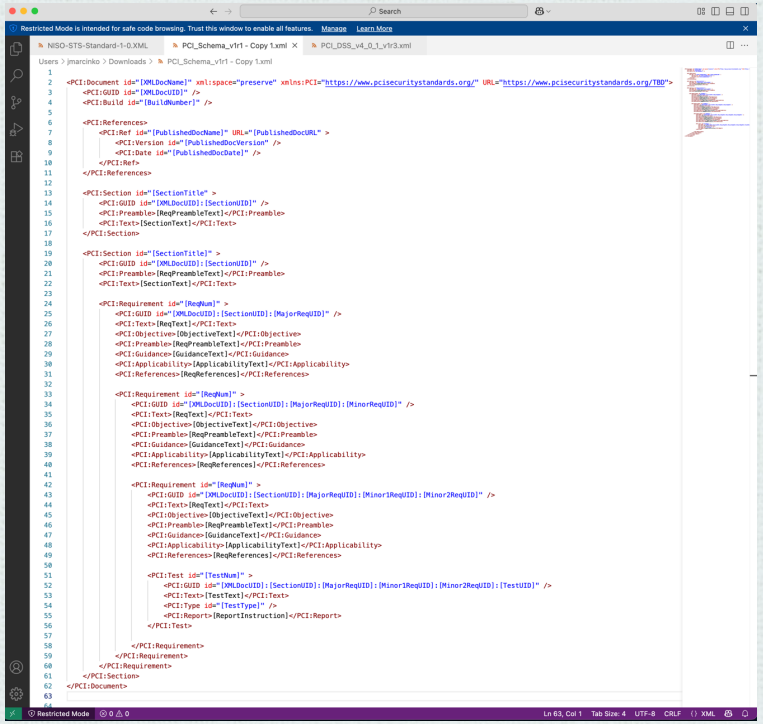
Cardholder data and sensitive authentication data are considered account data and are defined as follows:

Table 2. Account Data

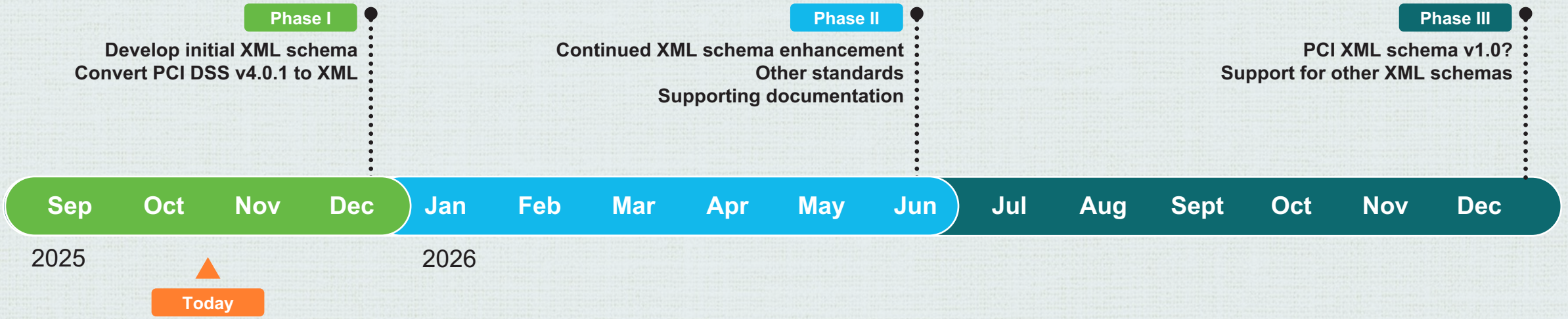
Account Data	
Cardholder Data includes:	**Sensitive Authentication Data includes:**
• Primary Account Number (PAN) • Cardholder Name • Expiration Date • Service Code	• Full track data (magnetic-stripe data or equivalent on a chip) • Card verification code • PINs/PIN blocks

PCI DSS requirements apply to entities with environments where account data (cardholder data and/or sensitive authentication data) is stored, processed, or transmitted, and entities with environments that can impact the security of cardholder data and/or sensitive authentication data. Some PCI DSS requirements may also apply to entities with environments that do not store, process, or transmit account data—for example, entities that outsource payment operations or management of their cardholder data environment (CDE).[1] Entities that outsource their payment environments or payment operations to third parties remain responsible for ensuring that the account data is protected by the third party per applicable PCI DSS requirements.

[1] In accordance with those organizations that manage compliance programs (such as payment brands and acquirers); entities should contact these organizations for more details.



Timelines



Note: Timelines and deliverables are subject to change.

Questions or Comments?

modernization@pcisecuritystandards.org

PCI Security Standards Council

THANK YOU!

PCI Security Standards Council