

Using and Assessing the Standard



John Elliott

PRIVACY, PAYMENTS, SECURITY AND RISK SPECIALIST

@withoutfire www.withoutfire.com



The Standard



How the standard is structured

How the standard is assessed

- Testing procedures

Reporting evidence

Resolving disputes with your assessor

What if you can't comply?



Protecting Diamonds From Pirates



Protecting the Diamonds

Let's design a security standard that protects the diamonds from the pirates ...

Pirate Control Initiative – Diamond Security Standard



I don't like the sound of that!



Protecting the Diamonds

**Give awareness training
to the diamonds**

**Install watchtowers and
searchlights**

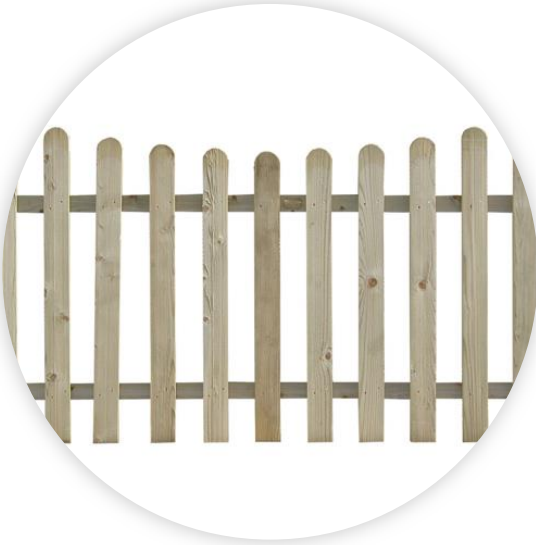
**Put land mines on the
beach**

**Deploy mines around the
island**

Build a fence



Build a Fence



or



Build a Fence

1.1 Build a fence that restricts pirates from entering the Controlled Diamond Environment (CDE)

1.1.1 Ensure fence is pirate-resistant

1.1.2 Ensure fence completely encircles CDE

1.1.3 Ensure fence is buried 1m below ground

1.2 Ensure all fence doors prevent pirates from entering the CDE through the door



But What Does
It Mean?

1.1.1 Ensure fence is pirate-resistant

Pirates carry very sharp swords and they really like diamonds. A soft fence made out of wood will easily be cut by a pirate. Fences should be made of a material – typically metal – that can resist a pirate's sword hacking at the fence for a considerable period of time

The intent of the requirement



How Would You Test?



1.1.1 Ensure fence is pirate-resistant

- a) Examine test certificate from manufacturer
- b) Stand behind fence holding a diamond shouting “here Mr. Pirate”, validate it takes the Pirate more than 120 minutes to cut through the fence
- c) Try cutting the fence with your penknife



Components of a Standard

1.1.2 Ensure fence is pirate-resistant

Requirement

Pirates carry very sharp swords and they really like diamonds. A soft fence made out of wood will easily be cut by a pirate. Fences should be made of a material – typically metal – that can resist a pirate’s sword hacking at the fence for a considerable period of time

Intent

- a) Examine test certificate from manufacturer
- b) Stand behind fence holding a diamond shouting “here Mr Pirate”, validate it takes the Pirate more than 120 minutes to cut through the fence
- c) Try cutting the fence with your penknife

Testing Procedure



Components of a Standard

6.4.3 Production data (live PANs) are not used for testing or development

Requirement

Security controls are usually not as stringent in test or development environments. Use of production data provides malicious individuals with the opportunity to gain unauthorized access to production data (cardholder data)

Intent

- a) Observe testing processes and interview personnel to verify procedures are in place to ensure production data (live PANs) are not used for testing or development
- b) Examine a sample of test data to verify production data (live PANs) is not used for testing or development

Testing Procedure



PCI DSS Requirements	Testing Procedures	Guidance
6.4.2 Separation of duties between development/test and production environments	6.4.2 Observe processes and interview personnel assigned to development/test environments and personnel assigned to production environments to verify that separation of duties is in place between development/test environments and the production environment.	<p>Reducing the number of personnel with access to the production environment and cardholder data minimizes risk and helps ensure that access is limited to those individuals with a business need to know.</p> <p>The intent of this requirement is to separate development and test functions from production functions. For example, a developer may use an administrator-level account with elevated privileges in the development environment, and have a separate account with user-level access to the production environment.</p>
6.4.3 Production data (live PANs) are not used for testing or development	6.4.3.a Observe testing processes and interview personnel to verify procedures are in place to ensure production data (live PANs) are not used for testing or development.	<p>Security controls are usually not as stringent in test or development environments. Use of production data provides malicious individuals with the opportunity to gain unauthorized access to production data (cardholder data).</p>
	6.4.3.b Examine a sample of test data to verify production data (live PANs) is not used for testing or development.	
6.4.4 Removal of test data and accounts from system components before the system becomes active / goes into production.	6.4.4.a Observe testing processes and interview personnel to verify test data and accounts are removed before a production system becomes active.	<p>Test data and accounts should be removed before the system component becomes active (in production), since these items may give away information about the functioning of the application or system. Possession of such information could facilitate compromise of the system and related cardholder data.</p>
	6.4.4.b Examine a sample of data and accounts from production systems recently installed or updated to verify test data and accounts are removed before the system becomes active.	



PCI DSS Requirements	Testing Procedures	Guidance
6.4.3 Production data (live PANs) are not used for testing or development	6.4.3.a Observe testing processes and interview personnel to verify procedures are in place to ensure production data (live PANs) are not used for testing or development.	Security controls are usually not as stringent in test or development environments. Use of production data provides malicious individuals with the opportunity to gain unauthorized access to production data (cardholder data).
	6.4.3.b Examine a sample of test data to verify production data (live PANs) is not used for testing or development.	



6.4.3.a Observe testing processes and interview personnel to verify procedures are in place to ensure production data (live PANs) are not used for testing or development.

6.4.3.b Examine a sample of test data to verify production data (live PANs) is not used for testing or development.

Report on Compliance



PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
6.4.3 Production data (live PANs) are not used for testing or development.			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.a Observe testing processes and interview personnel to verify procedures are in place to ensure production data (live PANs) are not used for testing or development.	Identify the responsible personnel interviewed who confirm that procedures are in place to ensure production data (live PANs) are not used for testing or development.	<Report Findings Here>					
	Describe how testing processes were observed to verify procedures are in place to ensure production data (live PANs) are not used for testing.	<Report Findings Here>					
	Describe how testing processes were observed to verify procedures are in place to ensure production data (live PANs) are not used for development.	<Report Findings Here>					
6.4.3.b Examine a sample of test data to verify production data (live PANs) is not used for testing or development.	Describe how a sample of test data was examined to verify production data (live PANs) is not used for testing.	<Report Findings Here>					



Report on Compliance



PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
6.4.3 Production data (live PANs) are not used for testing or development.			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.a Observe testing processes and interview personnel to verify procedures are in place to ensure production data (live PANs) are not used for testing or development.	Identify the responsible personnel interviewed who confirm that procedures are in place to ensure production data (live PANs) are not used for testing or development.	<Report Findings Here>					
	Describe how testing processes were observed to verify procedures are in place to ensure production data (live PANs) are not used for testing.	<Report Findings Here>					
	Describe how testing processes were observed to verify procedures are in place to ensure production data (live PANs) are not used for development.	<Report Findings Here>					
6.4.3.b Examine a sample of test data to verify production data (live PANs) is not used for testing or development.	Describe how a sample of test data was examined to verify production data (live PANs) is not used for testing.	<Report Findings Here>					



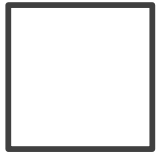
Report on Compliance



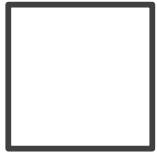
PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
6.4.3 Production data (live PANs) are not used for testing or development.			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.a Observe testing processes and interview personnel to verify procedures are in place to ensure production data (live PANs) are not used for testing or development.	Identify the responsible personnel interviewed who confirm that procedures are in place to ensure production data (live PANs) are not used for testing or development.	<Report Findings Here>					
	Describe how testing processes were observed to verify procedures are in place to ensure production data (live PANs) are not used for testing.	<Report Findings Here>					
	Describe how testing processes were observed to verify procedures are in place to ensure production data (live PANs) are not used for development.	<Report Findings Here>					
6.4.3.b Examine a sample of test data to verify production data (live PANs) is not used for testing or development.	Describe how a sample of test data was examined to verify production data (live PANs) is not used for testing.	<Report Findings Here>					



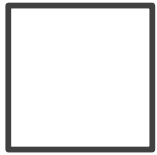
Assessment Findings



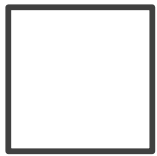
In place: Evidence found that the requirement is in place



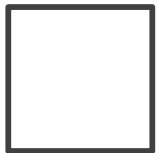
In place with CCW: Compensating controls used



N/A: The assessor confirms this requirement is not applicable



Not tested: The assessor didn't test this requirement



Not in place: No evidence that it is in place



Report on Compliance



PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
6.4.3 Production data (live PANs) are not used for testing or development.			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.a Observe testing processes and interview personnel to verify procedures are in place to ensure production data (live PANs) are not used for testing or development.	Identify the responsible personnel interviewed who confirm that procedures are in place to ensure production data (live PANs) are not used for testing or development.	<Report Findings Here>					
	Describe how testing processes were observed to verify procedures are in place to ensure production data (live PANs) are not used for testing.	<Report Findings Here>					
	Describe how testing processes were observed to verify procedures are in place to ensure production data (live PANs) are not used for development.	<Report Findings Here>					
6.4.3.b Examine a sample of test data to verify production data (live PANs) is not used for testing or development.	Describe how a sample of test data was examined to verify production data (live PANs) is not used for testing.	<Report Findings Here>					



PCI DSS Requirements	Testing Procedures	Guidance
----------------------	--------------------	----------

6.4.3.a Observe testing processes and interview personnel to verify procedures are in place to ensure production data (live PANs) are not used for testing or development.

6.4.3.b Examine a sample of test data to verify production data (live PANs) is not used for testing or development.

Report on Compliance



PCI DSS Requirements and Testing Procedures

6.4.3 Production data (live PANs)

6.4.3.a Observe testing processes to verify procedures are in place to ensure production data (live PANs) are not used for testing or development.

6.4.3.b Examine a sample of testing data to verify production data (live PANs) are not used for testing or development.

Identify the responsible personnel interviewed who confirm that procedures are in place to ensure production data (live PANs) are not used for testing or development.

Describe how testing processes were observed to verify procedures are in place to ensure production data (live PANs) are **not used for testing.**

Describe how testing processes were observed to verify procedures are in place to ensure production data (live PANs) are **not used for development.**

Assessment Findings

(Check one)

N/A	Not Tested	Not in Place
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



Report on Compliance



PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
6.4.3 Production data (live PANs) are not used for testing or development.			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<div>Interviewed Person_7 and Person_10. Both confirmed live PANs not used, test PANs have been made available by the acquirer and these are in use.</div>		Interviewed Person_7 and Person_10. Both confirmed live PANs not used, test PANs have been made available by the acquirer and these are in use.	<Report Findings Here>				
		Interviewed Person_7 and Person_10. Both confirmed live PANs not used, test PANs have been made available by the acquirer and these are in use.	<Report Findings Here>				
		Interviewed Person_7 and Person_10. Both confirmed live PANs not used, test PANs have been made available by the acquirer and these are in use.	<Report Findings Here>				
		Interviewed Person_7 and Person_10. Both confirmed live PANs not used, test PANs have been made available by the acquirer and these are in use.	<Report Findings Here>				
used for testing or development.	testing.						



Report on Compliance



PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
6.4.3 Production data (live PANs) are not used for testing or development.			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.a Observe testing processes and interview personnel to verify procedures are in place to ensure production data (live PANs) are not used for testing or development.	Identify the responsible personnel interviewed who confirm that procedures are in place to ensure production data (live PANs) are not used for testing or development.	Interviewed Person_7 and Person_10. Both confirmed live PANs not used, test PANs have been made available by the acquirer and these are in use.					
<div>Validated automated test scripts in Selenium. Only acquirer test PANs were present.</div>			<Report Findings Here>				
			<Report Findings Here>				
			<Report Findings Here>				



Help with Interpretation



Sources of Interpretation



PCI SSC
Guidance



PCI SSC
FAQs



The Internet



When There is a Difference of Opinion



PCI SSC
Guidance

AND



PCI SSC
FAQs

WILL



Usually make
a QSA happy!





Lots of PCI DSS content on the Internet

Be careful!

- Standard changes
- Technology changes

Many inaccuracies

- Not all Gurus are ...
- Won't persuade your QSA



Compensating Controls: When You Can't Comply with a Requirement



When You Can't Comply

**Legitimate Technical
Constraints**

**Documented Business
Constraints**



Appendix B: Compensating Controls

Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls.

Compensating controls must satisfy the following criteria:

1. Meet the intent and rigor of the original PCI DSS requirement.
2. Provide a similar level of defense as the original PCI DSS requirement, such that the compensating control sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against. (See *Guidance Column* for the intent of each PCI DSS requirement.)
3. Be "above and beyond" other PCI DSS requirements. (Simply being in compliance with other PCI DSS requirements is not a compensating control.)

When evaluating "above and beyond" for compensating controls, consider the following:

Note: The items at a) through c) below are intended as examples only. All compensating controls must be reviewed and validated for sufficiency by the assessor who conducts the PCI DSS review. The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control. Companies should be aware that a particular compensating control will not be effective in all environments.

- a) Existing PCI DSS requirements CANNOT be considered as compensating controls if they are already required for the item under review. For example, passwords for non-console administrative access must be sent encrypted to mitigate the risk of intercepting clear-text administrative passwords. An entity cannot use other PCI DSS password requirements (intruder lockout, complex passwords, etc.) to compensate for lack of encrypted passwords, since those other password requirements do not mitigate the risk of interception of clear-text passwords. Also, the other password controls are already PCI DSS requirements for the item under review (passwords).
 - b) Existing PCI DSS requirements MAY be considered as compensating controls if they are required for another area, but are not required for the item under review.
 - c) Existing PCI DSS requirements may be combined with new controls to become a compensating control. For example, if a company is unable to render cardholder data unreadable per Requirement 3.4 (for example, by encryption), a compensating control could consist of a device or combination of devices, applications, and controls that address all of the following: (1) internal network segmentation; (2) IP address or MAC address filtering; and (3) one-time passwords.
4. Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement

The assessor is required to thoroughly evaluate compensating controls during each annual PCI DSS assessment to validate that each compensating control adequately addresses the risk the original PCI DSS requirement was designed to address, per items 1-4 above. To maintain compliance, processes and controls must be in place to ensure compensating controls remain effective after the assessment is complete.

“Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to **legitimate technical** or **documented business** constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls.”



Appendix B: Compensating Controls

Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls.

Compensating controls must satisfy the following criteria:

1. Meet the intent and rigor of the original PCI DSS requirement.
2. Provide a similar level of defense as the original PCI DSS requirement, such that the compensating control sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against. (See *Guidance Column* for the intent of each PCI DSS requirement.)
3. Be "above and beyond" other PCI DSS requirements. (Simply being in compliance with other PCI DSS requirements is not a compensating control.)

When evaluating "above and beyond" for compensating controls, consider the following:

Note: The items at a) through c) below are intended as examples only. All compensating controls must be reviewed and validated for sufficiency by the assessor who conducts the PCI DSS review. The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control. Companies should be aware that a particular compensating control will not be effective in all environments.

- a) Existing PCI DSS requirements CANNOT be considered as compensating controls if they are already required for the item under review. For example, passwords for non-console administrative access must be sent encrypted to mitigate the risk of intercepting clear-text administrative passwords. An entity cannot use other PCI DSS password requirements (intruder lockout, complex passwords, etc.) to compensate for lack of encrypted passwords, since those other password requirements do not mitigate the risk of interception of clear-text passwords. Also, the other password controls are already PCI DSS requirements for the item under review (passwords).
 - b) Existing PCI DSS requirements MAY be considered as compensating controls if they are required for another area, but are not required for the item under review.
 - c) Existing PCI DSS requirements may be combined with new controls to become a compensating control. For example, if a company is unable to render cardholder data unreadable per Requirement 3.4 (for example, by encryption), a compensating control could consist of a device or combination of devices, applications, and controls that address all of the following: (1) internal network segmentation; (2) IP address or MAC address filtering; and (3) one-time passwords.
4. Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement

The assessor is required to thoroughly evaluate compensating controls during each annual PCI DSS assessment to validate that each compensating control adequately addresses the risk the original PCI DSS requirement was designed to address, per items 1-4 above. To maintain compliance, processes and controls must be in place to ensure compensating controls remain effective after the assessment is complete.

Appendix C: Compensating Controls Worksheet

Use this worksheet to define compensating controls for any requirement where compensating controls are used to meet a PCI DSS requirement. Note that compensating controls should also be documented in the Report on Compliance in the corresponding PCI DSS requirement section.

Note: Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance.

Requirement Number and Definition:

	Information Required	Explanation
1. Constraints	List constraints precluding compliance with the original requirement.	
2. Objective	Define the objective of the original control; identify the objective met by the compensating control.	
3. Identified Risk	Identify any additional risk posed by the lack of the original control.	
4. Definition of Compensating Controls	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	
6. Maintenance	Define process and controls in place to maintain compensating controls.	



Appendix B: Compensating Controls

Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls.

Compensating controls must satisfy the following criteria:

1. Meet the intent and rigor of the original PCI DSS requirement.
2. Provide a similar level of defense as the original PCI DSS requirement, such that the control sufficiently offsets the risk that the original PCI DSS requirement was designed to address. (See *Guidance Column* for the intent of each PCI DSS requirement.)
3. Be "above and beyond" other PCI DSS requirements. (Simply being in compliance with other PCI DSS requirements is not a compensating control.)

When evaluating "above and beyond" for compensating controls, consider the following:

Note: The items at a) through c) below are intended as examples only. All compensating controls must be reviewed and validated for sufficiency by the assessor who conducts the PCI DSS assessment. The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the system. The assessor should be aware that a particular compensating control will not be effective in all environments.

- a) Existing PCI DSS requirements CANNOT be considered as compensating controls if they are already required for the item under review. For example, passwords for non-administrative access must be sent encrypted to mitigate the risk of interception of administrative passwords. An entity cannot use other PCI DSS password requirements (e.g., password lockout, complex passwords, etc.) to compensate for lack of encrypted passwords. Other password requirements do not mitigate the risk of interception of credentials if the other password controls are already PCI DSS requirements for the item under review (passwords).
 - b) Existing PCI DSS requirements MAY be considered as compensating controls if they are for another area, but are not required for the item under review.
 - c) Existing PCI DSS requirements may be combined with new controls to better address the risk. For example, if a company is unable to render cardholder data unreadable (Requirement 3.4 (for example, by encryption)), a compensating control could be implemented, such as a combination of devices, applications, and controls that address all of the following: (1) network segmentation; (2) IP address or MAC address filtering; and (3) other controls that address the risk.
4. Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.

The assessor is required to thoroughly evaluate compensating controls during each annual PCI DSS assessment to validate that each compensating control adequately addresses the risk the original PCI DSS requirement was designed to address, per items 1-4 above. To maintain compliance, processes and controls must be in place to ensure compensating controls remain effective after the assessment is complete.

Appendix C: Compensating Controls Worksheet

Use this worksheet to define compensating controls for any requirement where compensating controls are used to meet a PCI DSS requirement. Note that compensating controls should also be documented in the Report on Compliance in the corresponding PCI DSS requirement section.

Note: Only companies that have undertaken a risk analysis and have legitimate technological or business reasons for the use of compensating controls to achieve compliance.

Requirement 2.3

Encrypt all non-console administrative access using strong cryptography.

	Explanation
Existing compensating controls.	
If the original requirement is not met by the control.	
The risk posed by the control.	
Existing controls and how they address the risk of the original control and any compensating controls used.	
Controls in place to ensure compensating controls remain effective.	



Compensating Controls



1. Meet the intent and rigor of the original PCI DSS requirement.
2. Provide a similar level of defense as the original PCI DSS requirement, such that the compensating control sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against.
3. Be “above and beyond” other PCI DSS requirements.



Appendix C: Compensating Controls Worksheet

Use this worksheet to define compensating controls for any requirement where compensating controls are used to meet a PCI DSS requirement. Note that compensating controls should also be documented in the Report on Compliance in the corresponding PCI DSS requirement section.

Note: Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance.

Requirement Number and Definition:

	Information Required	Explanation
1. Constraints	List constraints precluding compliance with the original requirement.	
2. Objective	Define the objective of the original control; identify the objective met by the compensating control.	
3. Identified Risk	Identify any additional risk posed by the lack of the original control.	
4. Definition of Compensating Controls	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	
6. Maintenance	Define process and controls in place to maintain compensating controls.	



1. Constraints

List constraints precluding compliance with the original requirement.

2. Objective

Define the objective of the original control; identify the objective met by the compensating control.

3. Identified Risk

Identify any additional risk posed by the lack of the original control.

4. Definition of Compensating Control

Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.

5. Validation of Compensating Control

Define how the compensating controls were validated and tested.

6. Maintenance

Define process and controls in place to maintain compensating controls.



1. Constraints	List constraints precluding compliance with the original requirement.	Old switches in the CDE do not support any encrypted protocol for Admin login (Requirement 2.3)
2. Objective	Define the objective of the original control; identify the objective met by the compensating control.	Admin credentials for the switches on the network can not be intercepted or eavesdropped by a threat actor (TA)
3. Identified Risk	Identify any additional risk posed by the lack of the original control.	A TA with access to network traffic would be able to access a switch and monitor all traffic. But all PAN and credentials in use encrypted so limited risk.
4. Definition of Compensating Control	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	Management of switches restricted to single IP from a jump host. Admins must login to jump host within the CDE (with 2FA) and then telnet from jump host to switches.
5. Validation of Compensating Control	Define how the compensating controls were validated and tested.	Attempt to telnet to switches directly. Connections rejected.
6. Maintenance	Define process and controls in place to maintain compensating controls.	Standard build document for replacement switches. Attempts to Telnet switches run automatically every quarter alongside vulnerability scans



Some QSAs Have Problems with CCs



“Can not be used for Requirement Z”

“Only valid for X years”

- No limit
- Must be reviewed each year – is the constraint still valid?

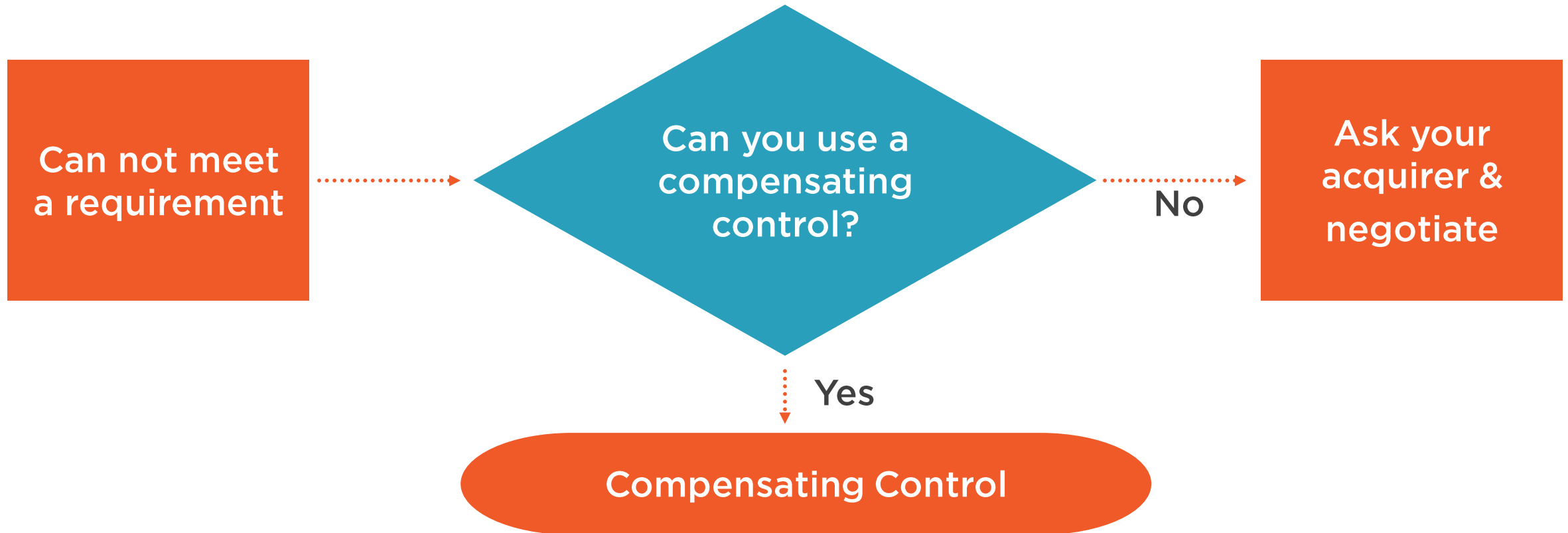
“Must be agreed with acquirer”

- No: It is the QSA's call

“Must be approved by the PCI SSC”

- No. FAQ 1046

Can't Meet a Requirement



Next: The Assessment

