The Customized Approach

John Elliott

Payments, Security, Privacy and Risk Specialist | PCIP

@withoutfire www.johnelliott.eu

How the Customized Approach Works

Requirements and Testing Procedures		Guidance
Defined Approach Requirements **5.2.2** The deployed anti-malware solution(s): ☐ Detects all known types of malware. ☐ Removes, blocks, or contains all known types of malware.	**Defined Approach Testing Procedures** **5.2.2** Examine vendor documentation and configurations of the anti-malware solution(s) to verify that the solution: ☐ Detects all known types of malware. ☐ Removes, blocks, or contains all known types of malware.	**Purpose** It is important to protect against all types and forms of malware to prevent unauthorized access. **Good Practice** Anti-malware solutions may include a combination of network-based controls, host-based controls, and endpoint security solutions. In addition to signature-based tools, capabilities used by modern anti-malware solutions include sandboxing, privilege escalation controls, and machine learning. Solution techniques include preventing malware from getting into the network and removing or containing malware that does get into the network. **Examples** Types of malware include, but are not limited to, viruses, Trojans, worms, spyware, ransomware, keyloggers, rootkits, malicious code, scripts, and links.
Customized Approach Objective Malware cannot execute or infect other system components.		

How the Customized Approach Works

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** It is important to protect against all types and forms of malware to prevent unauthorized access. **Good Practice** Anti-malware solutions may include a combination of network-based controls, host-based controls, and endpoint security solutions. In addition to signature-based tools, capabilities used by modern anti-malware solutions include sandboxing, privilege escalation controls, and machine learning. Solution techniques include preventing malware from getting into the network and removing or containing malware that does get into the network. **Examples** Types of malware include, but are not limited to, viruses, Trojans, worms, spyware, ransomware, keyloggers, rootkits, malicious code, scripts, and links.
5.2.2 The deployed anti-malware solution(s): □ Detects all known types of malware. □ Removes, blocks, or contains all known types of malware.	**5.2.2** Examine vendor documentation and configurations of the anti-malware solution(s) to verify that the solution: □ Detects all known types of malware. □ Removes, blocks, or contains all known types of malware.	
Customized Approach Objective Malware cannot execute or infect other system components.		

How the Customized Approach Works

Defined Approach

Objective

5.2.2 The deployed anti-malware solution(s):

- **Detects all known types of malware.**
- **Removes, blocks, or contains all known types of malware.**

Testing Procedure

Examine vendor documentation and configurations of the anti-malware solution(s) to verify that the solution:

- **Detects all known types of malware.**
- **Removes, blocks, or contains all known types of malware.**

Customized Approach

Objective

5.2.2 Malware cannot execute, or infect other system components.

An organization can select its own controls to meet the customized approach objective.

How the Customized Approach Works

Defined Approach

Objective

5.2.2 The deployed anti-malware solution(s):

- **Detects all known types of malware.**
- **Removes, blocks, or contains all known types of malware.**

Testing Procedure

Examine vendor documentation and configurations of the anti-malware solution(s) to verify that the solution:

- **Detects all known types of malware.**
- **Removes, blocks, or contains all known types of malware.**

Customized Approach

Objective

5.2.2 Malware cannot execute or infect other system components.

An organization deploys allow-listing to prevent all unknown software executing

How the Customized Approach Works

Defined Approach	Customized Approach
Objective 5.2.2 The deployed anti-malware solution(s): • Detects all known types of malware. • Removes, blocks, or contains all known types of malware. **Testing Procedure** Examine vendor documentation and configurations of the anti-malware solution(s) to verify that the solution: • Detects all known types of malware. • Removes, blocks, or contains all known types of malware.	**Objective** 5.2.2 Malware cannot execute or infect other system components.
For each requirement you can do this	**or this**

How the Customized Approach Works

Defined Approach	Customized Approach

Or, for any requirement you can do both:

- **Defined approach for one environment**
- **Customized approach for a different environment**

Customized Approach

Designed for “sophisticated” entities / organizations

Requires an assessor – QSA or ISA

Brands may make rules about this

Very new

Probably expensive

What About Compensating Controls?

Compensating Controls	Customized Approach

What About Compensating Controls?

Compensating Controls

When an organization cannot meet a requirement because of a legitimate and documented, business or technical reason.

Meets the intent of the defined approach requirement.

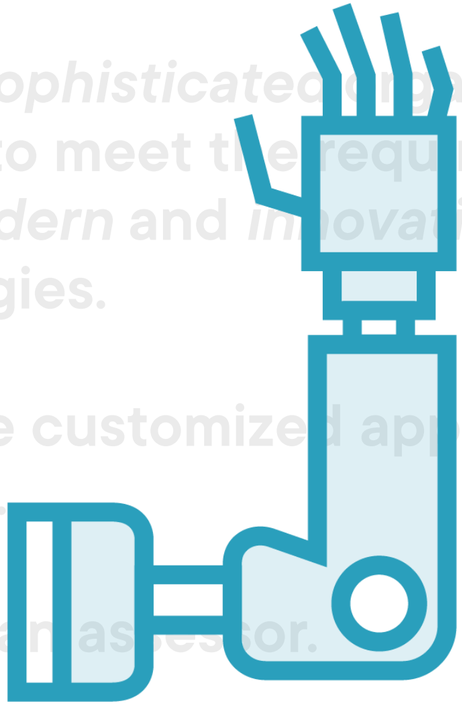
Does not require an assessor.

Customized Approach

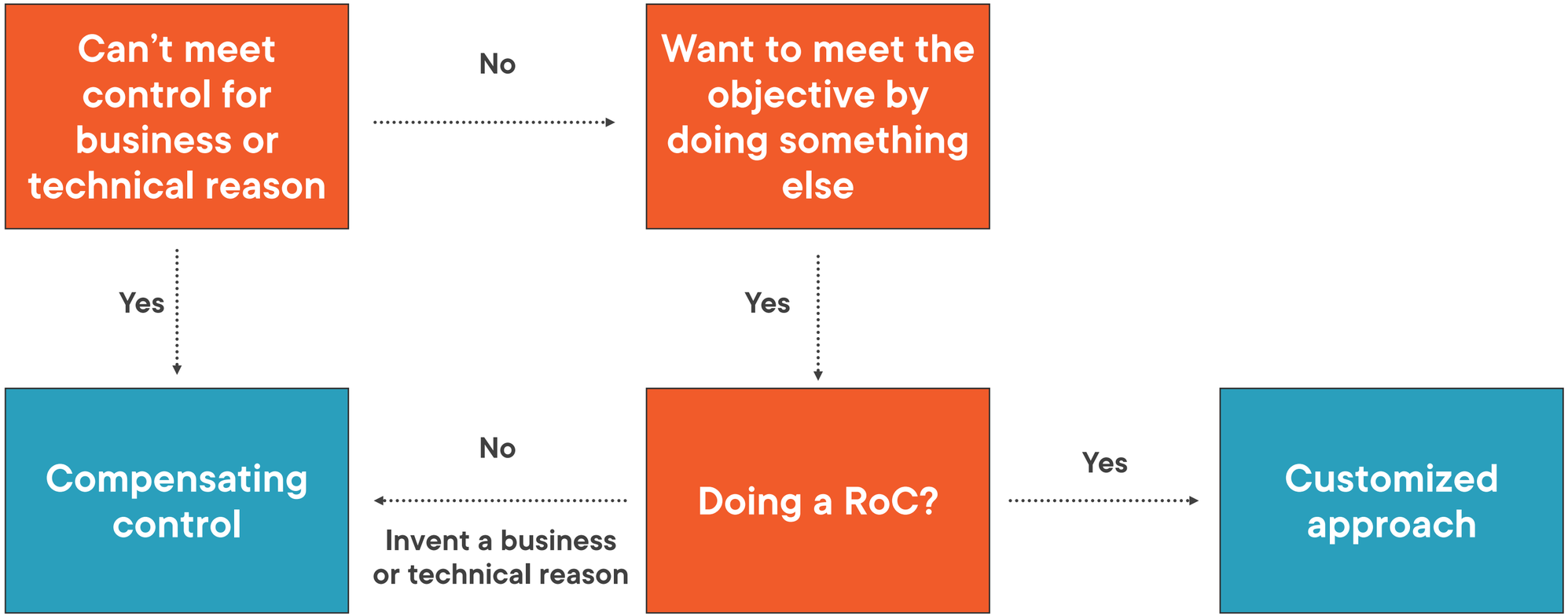
When a *sophisticated* organization chooses to meet the requirement using *modern* and *innovative* technologies.

Meets the customized approach objective.

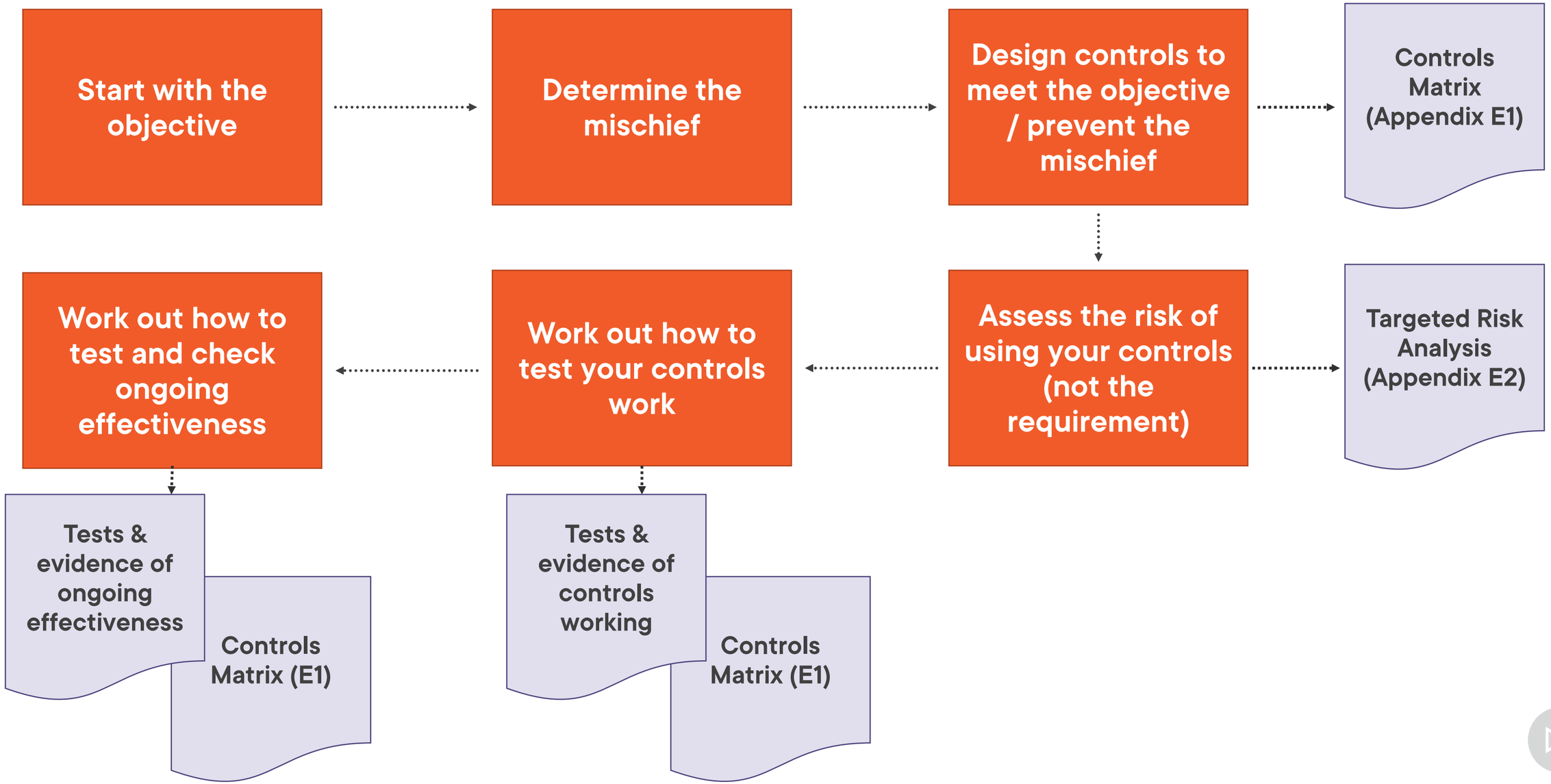
Requires an assessor.



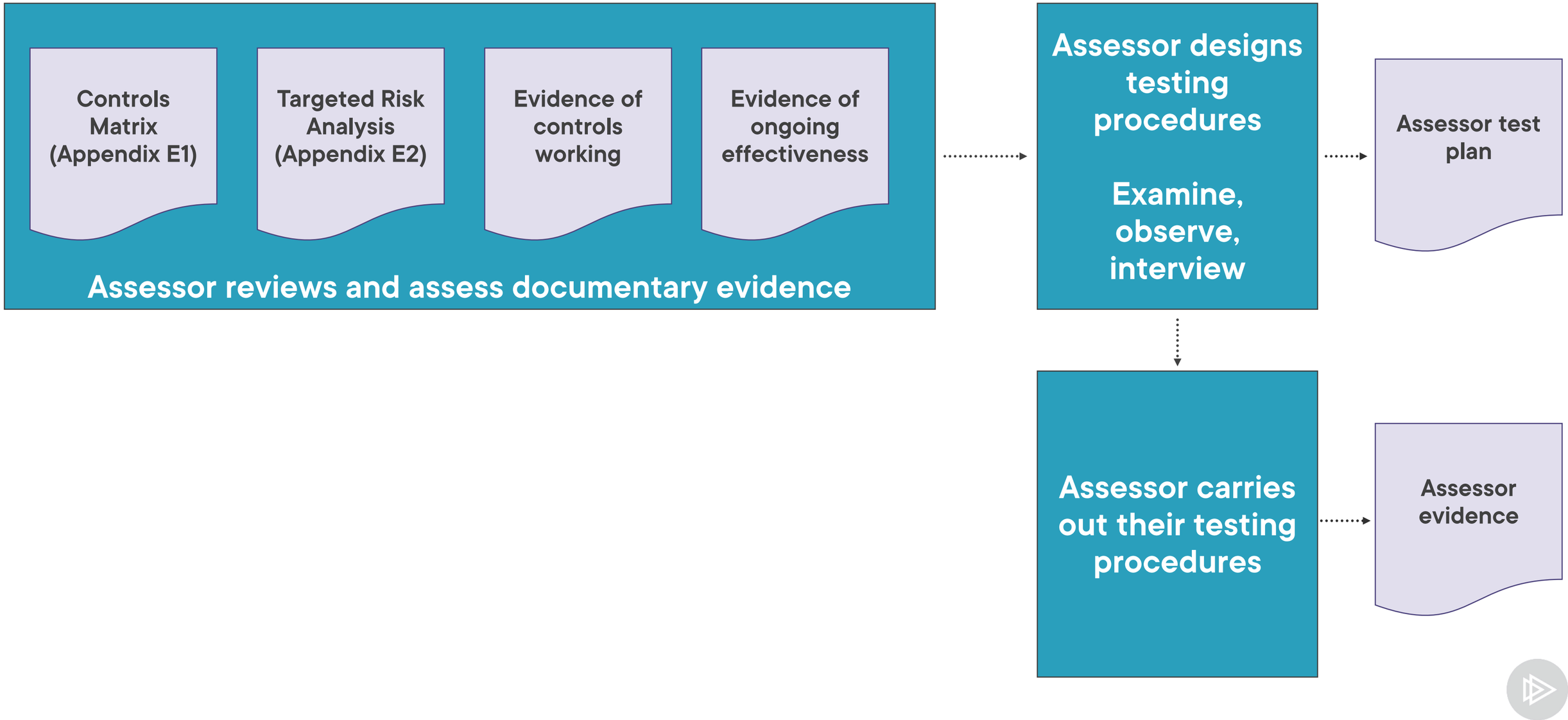
What Can You Use?



How to Do the Customized Approach



How It Will Be Assessed



Understanding Objectives and Mischief

Understanding Objectives

Prevent	**[Asset/s] cannot be [verb] by [descriptor]**
Do	**[Artefact/s] are [verb/s]**
Assure	**[Asset/s] are verified [periodically] [by quality] [to a standard]**

Understanding Objectives

Prevent	**[Asset/s] cannot be [verb] by [descriptor]**
Do	[Artefact/s] are [verb/s]
Assure	[Asset/s] are verified [periodically] [by quality] [to a standard]

Understanding Objectives

Prevent	**Cleartext PAN cannot be read or intercepted from any transmissions over open, public networks.**
Do	[Artefact/s] are [verb/s]
Assure	[Asset/s] are verified [periodically] [by quality] [to a standard]

Understanding Objectives

Prevent	[Asset/s] cannot be [verb] by [descriptor]
Do	[Artefact/s] are [verb/s]
Assure	[Asset/s] are verified [periodically] [by quality] [to a standard]

Understanding Objectives

Prevent	[Asset/s] cannot be [verb] by [descriptor]
Do	**Vulnerabilities and security weaknesses found while verifying system defenses are mitigated.**
Assure	[Asset/s] are verified [periodically] [by quality] [to a standard]

Understanding Objectives

Prevent	[Asset/s] cannot be [verb] by [descriptor]
Do	[Artefact/s] are [verb/s]
Assure	**[Asset/s] are verified [periodically] [by quality] [to a standard]**

Understanding Objectives

Prevent

[Asset/s] cannot be [verb] by [descriptor]

Do

[Artefact/s] are [verb/s]

Assure

The security posture of all system components is verified periodically using automated tools designed to detect vulnerabilities operating inside the network.

Understanding Objectives

Prevent	**[Asset/s] cannot be [verb] by [descriptor]**
Do	**[Artefact/s] are [verb/s]**
Assure	**[Asset/s] are verified [periodically] [by quality] [to a standard]**

Understanding Mischief

Objective	Opposite	Mischief	Consequence
All keys and certificates used to protect PAN during transmission are identified and confirmed as trusted.	All keys and certificates used to protect PAN during transmission are not identified and are untrusted.	A threat actor is able to substitute a key or certificate.	The threat actor will be able to intercept (attacker in the middle) encrypted transmissions and extract the plaintext PAN.

This is needed for the Targeted Risk Analysis

Two Standards in One

A prescriptive security standard

An objective-based security standard

PCI DSS Version 4.0 Resource Hub

PCI Data Security Standard (PCI DSS) is a global standard that provides a baseline of technical and operational requirements designed to protect account data. The next evolution of the standard- PCI DSS v4.0- is now available.

This PCI DSS Resource Hub provides links to both standard documents and educational resources to help organizations become familiar with PCI DSS v4.0. Make sure to subscribe to the PCI Perspectives Blog to stay up to date on all news from PCI SSC.

https://blog.pcisecuritystandards.org/pci-dss-v4-0-resource-hub