

Matt O'Connor

Director, Assessor Quality Management

John Bloomfield

Manager, Data Security Standards



All About INFI

Compensating Controls (CCs)

“Intended to help entities address the risk when there is a **technical** or **business** constraint that prevents meeting the PCI DSS requirement as stated”

Compensating Controls (CCs)

- Proactive
- Known business or technical constraint
- Cannot meet the requirement as stated
- Typically documented by the entity being assessed

Compensating Controls (CCs)

- Proactive
- Known business or technical constraint
- Cannot meet the requirement as stated
- Typically documented by the entity being assessed

Business convenience to please the customers is not a "constraint"

Poor planning is not a valid reason for use of a Compensating Control

Compensating Controls cannot be used with the Customized Approach



Clean Air Requirement

Staff members must cycle to and from work 5 days each week to limit air pollution

Clean Air Requirement

- **Fictitious Example**
 - Staff members must cycle to and from work 5 days each week to limit air pollution
- **In Place – Requirement met**
 - The staff member has been cycling to work continuously, 5 days a week, as evidenced by a recorded travel diary



Clean Air Requirement

- **Fictitious Example**
 - Staff members must cycle to and from work 5 days each week to limit air pollution
- **Not In Place – Requirement is not met**
 - The staff member has not cycled to work and has used their personal quad bike instead

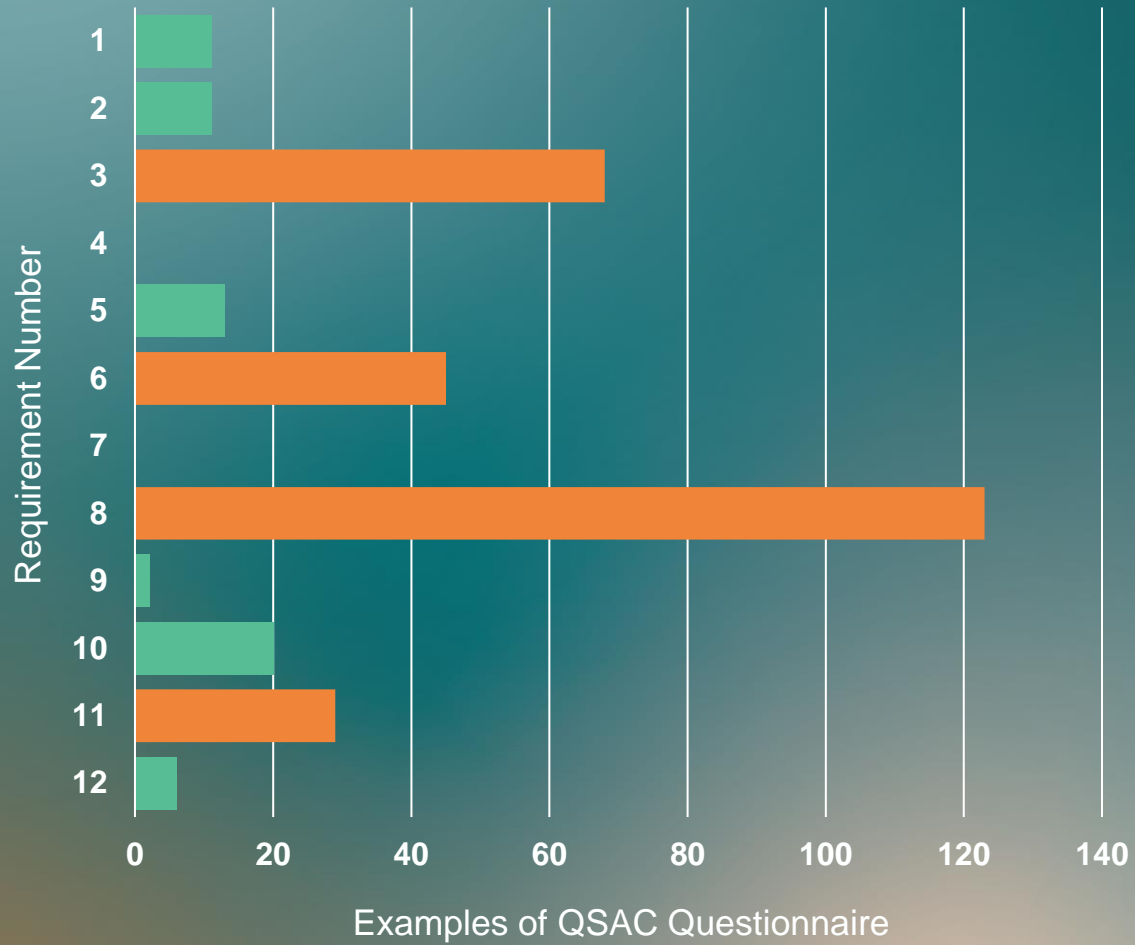


Clean Air Requirement

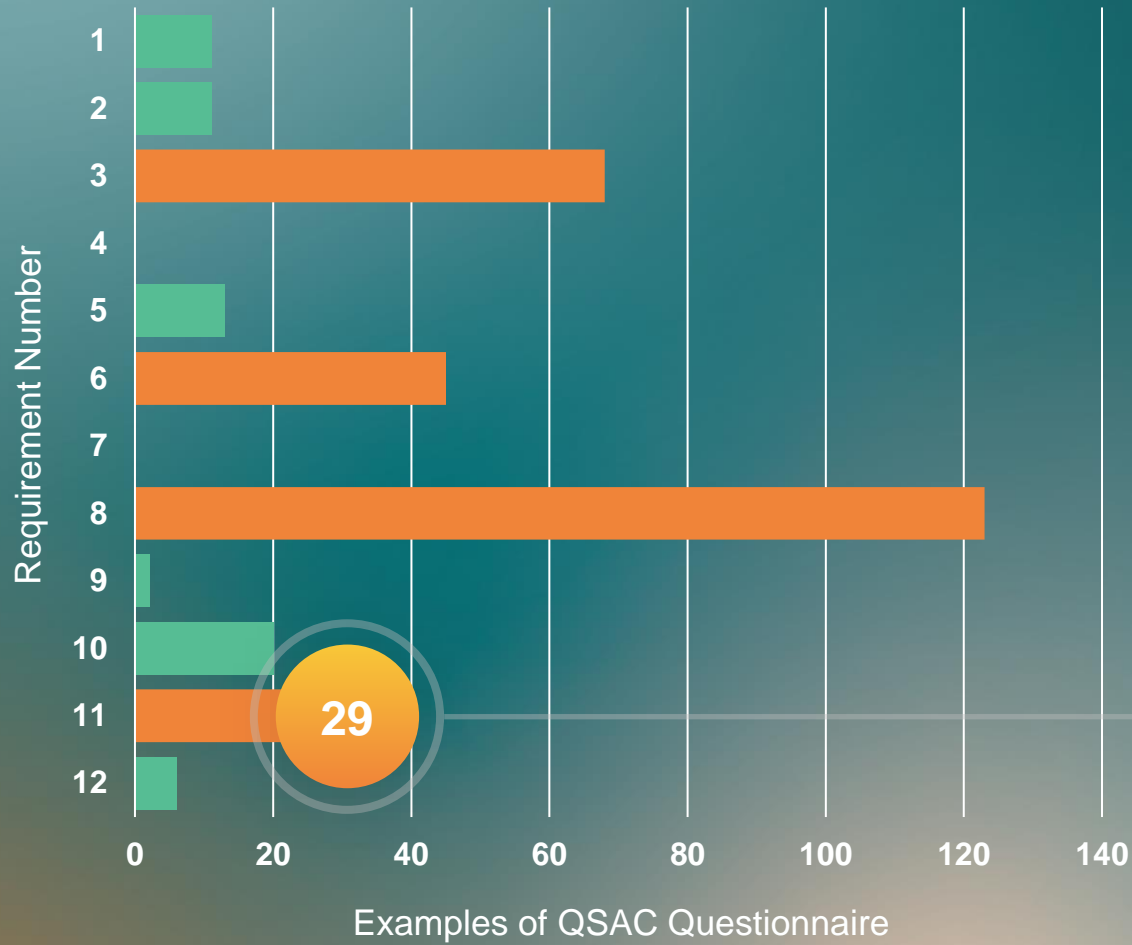
- **Fictitious Example**
 - Staff members must cycle to and from work 5 days each week to limit air pollution
- **In Place with Compensating Control**
 - The company provides a shuttle bus in bad weather



Compensating Controls (CCs)

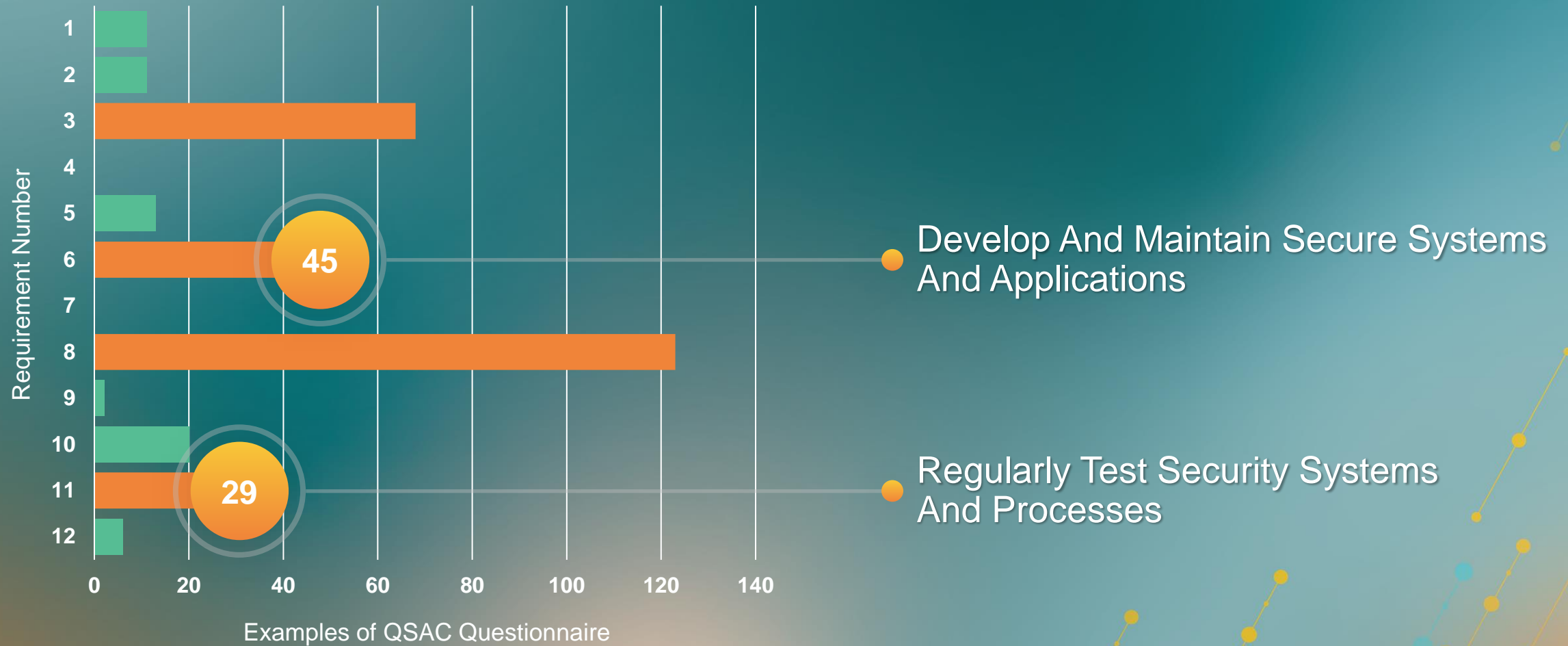


Compensating Controls (CCs)

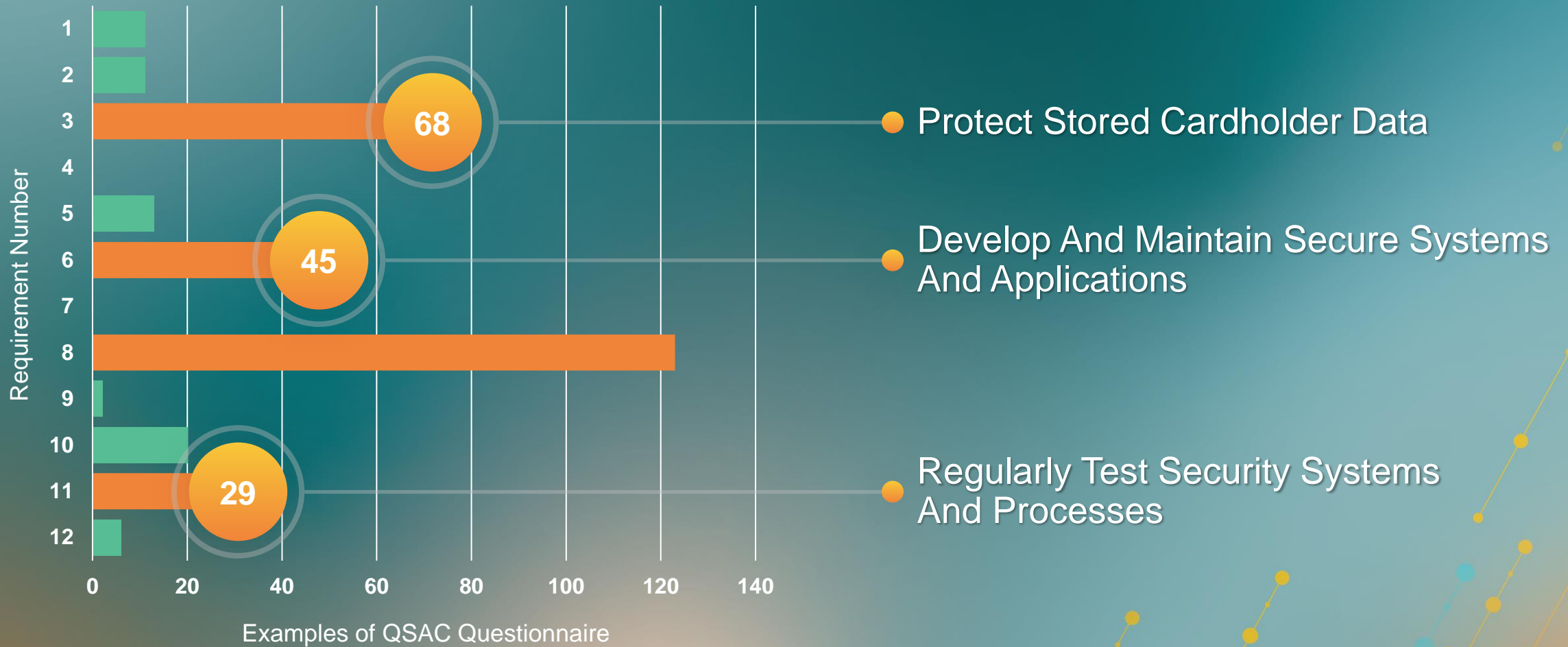


Regularly Test Security Systems And Processes

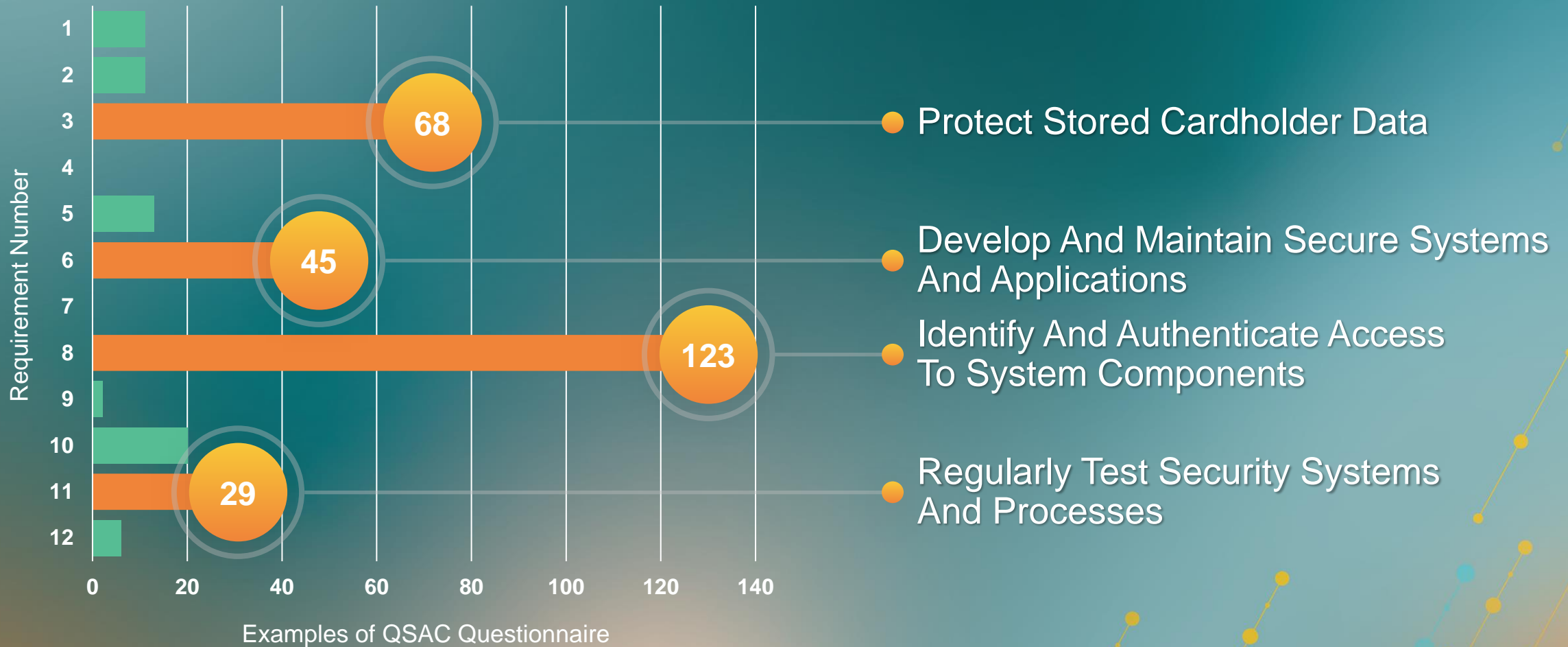
Compensating Controls (CCs)



Compensating Controls (CCs)



Compensating Controls (CCs)



Items Noted For Improvement (INFI)

“For internal use between the assessor and the assessed entity when a PCI DSS requirement was not initially met, but where the entity has taken steps to address the failure and ensure that the **requirement is met** going forward.”

Items Noted For Improvement (INFI)

- Reactive
- Lapse in control due to unforeseen or exceptional circumstance
- Has addressed cause of control lapse; requirement is now in place

Items Noted For Improvement (INFI)

- Reactive
- Lapse in control due to unforeseen or exceptional circumstance
- Has addressed cause of control lapse; requirement is now in place

**Poor planning is not a
valid reason for the
use of INFI**

Items Noted For Improvement (INFI)

- **Fictitious Example**
 - Staff members must cycle to and from work 5 days each week to limit air pollution
- **Compliant – with Items Noted For Improvement**
 - Following a puncture, a staff member could not cycle to work
 - The staff member subsequently bought a puncture repair kit





What if There Is a Legal Exception?

Legal Exception

- Where a legal exception means that the requirement(s) cannot be met:

<input type="checkbox"/>	<p>Compliant but with Legal exception: One or more assessed requirements in the ROC are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall COMPLIANT BUT WITH LEGAL EXCEPTION rating; thereby <i>(Merchant Company Name)</i> has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction.</p> <p>This option requires additional review from the entity to which this AOC will be submitted.</p> <p><i>If selected, complete the following:</i></p>
Affected Requirement	Details of how legal constraint prevents requirement from being met

An Example Using a PCI DSS Requirement



An Example Using a PCI DSS Requirement

PCI DSS v4.0 - DEFINED APPROACH REQUIREMENTS

11.3.2 External vulnerability scans are performed as follows:

- At least once every three months.
- By a PCI SSC Approved Scanning Vendor (ASV).
- Vulnerabilities are resolved and *ASV Program Guide* requirements for a passing scan are met.
- Rescans are performed as needed to confirm that vulnerabilities are resolved per the *ASV Program Guide* requirements for a passing scan.

Which One Do I Use When?

- **Compensating Control (CC)**
 - Proactive
 - Known business or technical constraint
 - Cannot meet the requirement; alternative controls implemented

Business convenience to please the customers is not a "constraint"

Poor planning is not a valid reason for use of a Compensating Control

Compensating Controls cannot be used with the Customized Approach

Which One Do I Use When?

- **Items Noted for Improvement (INFI)**
 - Reactive
 - Lapse in control due to unforeseen or exceptional circumstance
 - Has addressed cause of control lapse; requirement is now in place

**Temporarily “Not In Place”
but fixed and future-proofed**

**Poor planning is not a valid
reason for the use of INFI**

Which One Do I Use When?

- **Requirement: 11.3.2**
 - **In Place**
The entity can evidence a passing scan at least once every three months
 - **Not In Place**
The entity cannot evidence a passing scan at least once every three months

Which One Do I Use When?

- **Requirement: 11.3.2 - Examples
In Place with Compensating Control**



Which One Do I Use When?

- Requirement: 11.3.2 - Examples

In Place with Items Noted For Improvement (INFI)



Common INFI Questions

- Will PCI SSC provide an INFI template?

Common INFI Questions

- Will PCI SSC provide an INFI template?
- Should QSAs complete INFI for each assessment?

Common INFI Questions

- Will PCI SSC provide an INFI template?
- Should QSAs complete INFI for each assessment?
- Who must sign the INFI worksheet?

Common INFI Questions

- Will PCI SSC provide an INFI template?
- Should QSAs complete INFI for each assessment?
- Who must sign the INFI worksheet?
- SAQs?

Common INFI Questions

- Will PCI SSC provide an INFI template?
- Should QSAs complete INFI for each assessment?
- Who must sign the INFI worksheet?
- SAQs?
- ISAs?

Common INFI Questions

- Will PCI SSC provide an INFI template?
- Should QSAs complete INFI for each assessment?
- Who must sign the INFI worksheet?
- SAQs?
- ISAs?
- Use with v3.2.1?

The background features a blurred image of hands typing on a keyboard, overlaid with a complex network of glowing blue and yellow nodes connected by thin lines. The overall color palette is dominated by teal and blue tones, with a curved orange gradient at the bottom.

~~All About INFI~~ It Is Not Just About INFI