Tom White

Senior Manager, Content Development

Emma Sutcliffe

Senior Vice President, Standards

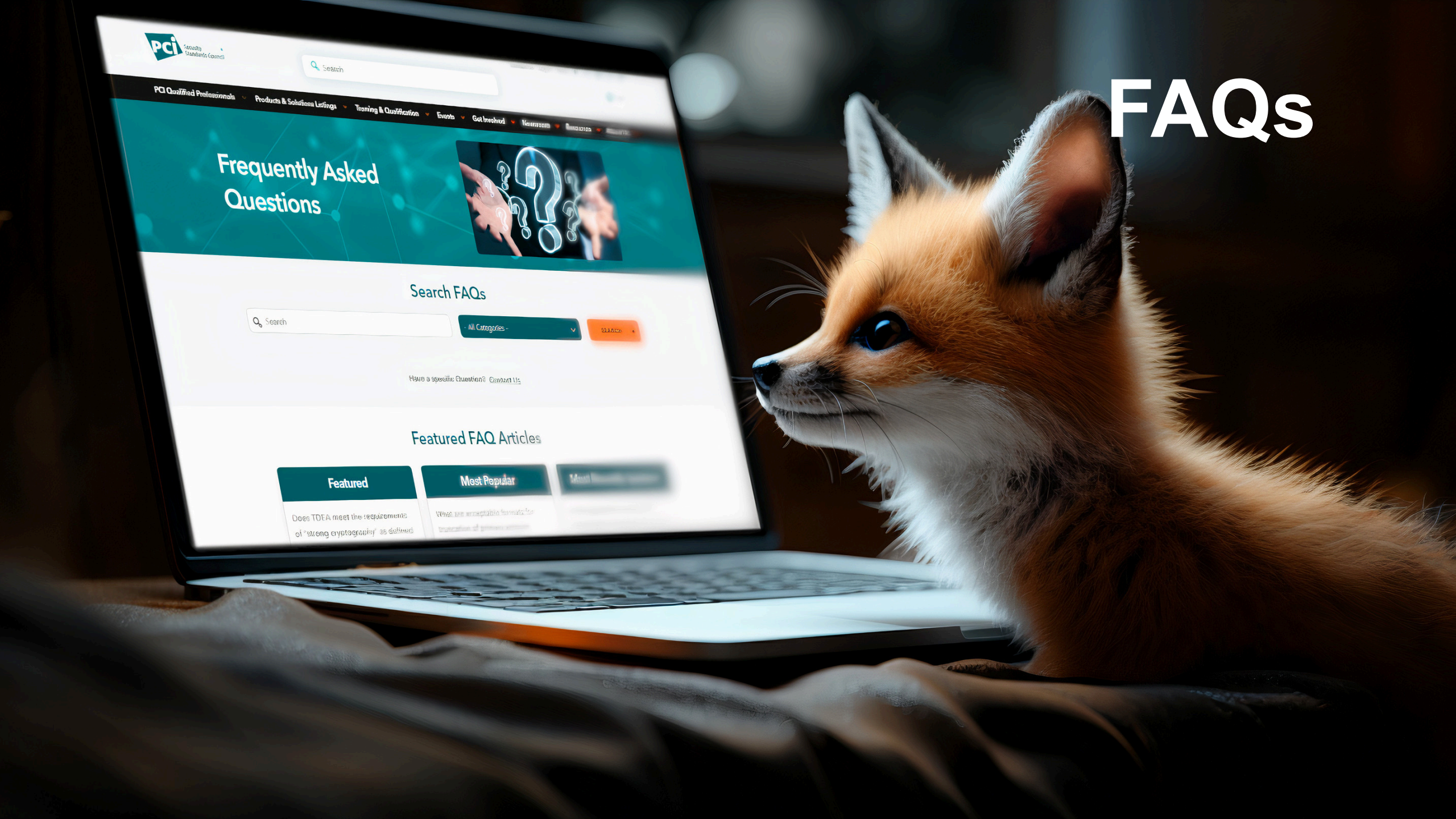
Lauren Holloway

Director, Data Security Standards

PCI Security Standards Council

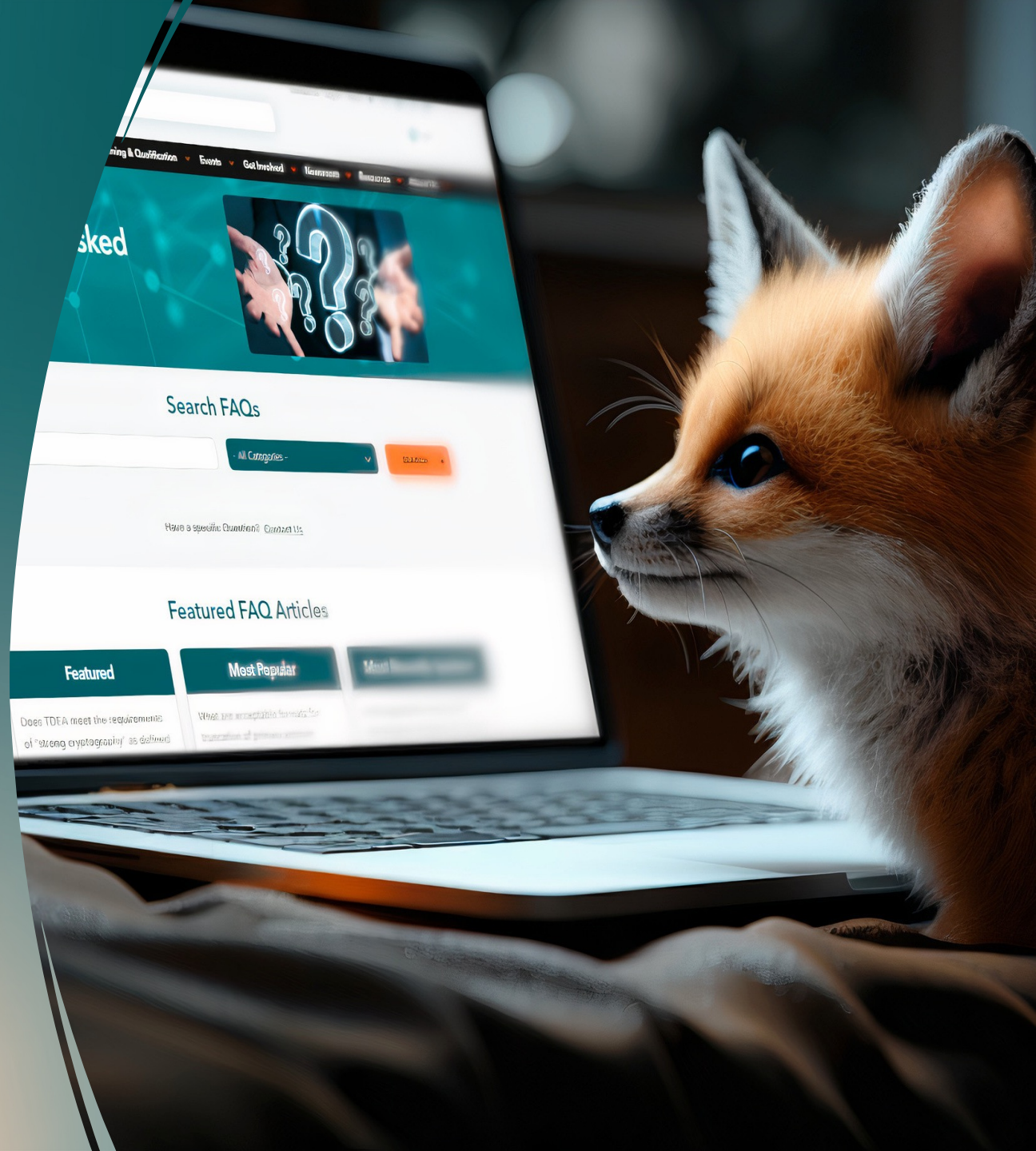
What's New?

PCI DSS v4.0 - Part 1


FAQs
Frequently Asked Questions
Search FAQs
Search
Featured FAQ Articles
Featured
Most Popular

FAQs

- Is TDEA 'strong cryptography' as defined in PCI DSS?
- What does 'duly authorized officer' mean?
- How should payment terminals be considered during an assessment?
- Can assessors rely on other types of assessments?
- Is sampling allowed in PCI DSS v4.0?



PCI Security Standards Council


Self-Assessment
Questionnaires

Targeted Risk Analyses

Targeted Risk Analyses

- Required for:
  - Customized Approach
  - 'Periodic' requirements
- Evidence documented and reviewed during assessments
- No 'organization-wide' risk assessment requirement

PCI Security Standards Council

Passwords


Multi-Factor
Authentication


Summary

PCI Security Standards Council

All About INFI

PCI DSS v4.0 - Part 2

Items Noted For Improvement (INFI)

Intended to help entities work towards security as a continuous process.

Used when the entity or assessor identifies one or more items that **required corrective action** for the requirement to be considered In Place.

PCI Security Standards Council

Items Noted For Improvement (INFI) Characteristics

- Reactive
- Lapse in control due to unforeseen or exceptional circumstance
- Entity has addressed cause of control lapse
- Requirement verified by assessor as being in place
- Entity has taken steps to prevent reoccurrence of control lapse
- Documented by Assessor during assessment

Items Noted For Improvement (INFI) Characteristics

- Reactive
- Lapse in control due to unforeseen or exceptional circumstance
- Entity has addressed cause of control lapse
- Requirement verified by assessor as being in place
- Entity has taken steps to prevent reoccurrence of control lapse
- Documented by Assessor during assessment

INFI is NOT used to justify poor security practices

PCI Security Standards Council

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"

PCI Security Standards Council

Compensating Controls (CCs) Characteristics

- Proactive
- Known business or technical constraint
- Cannot meet the requirement as stated
- Additional controls put in place to mitigate risk
- Typically documented by the entity being assessed

Compensating Controls (CCs) Characteristics

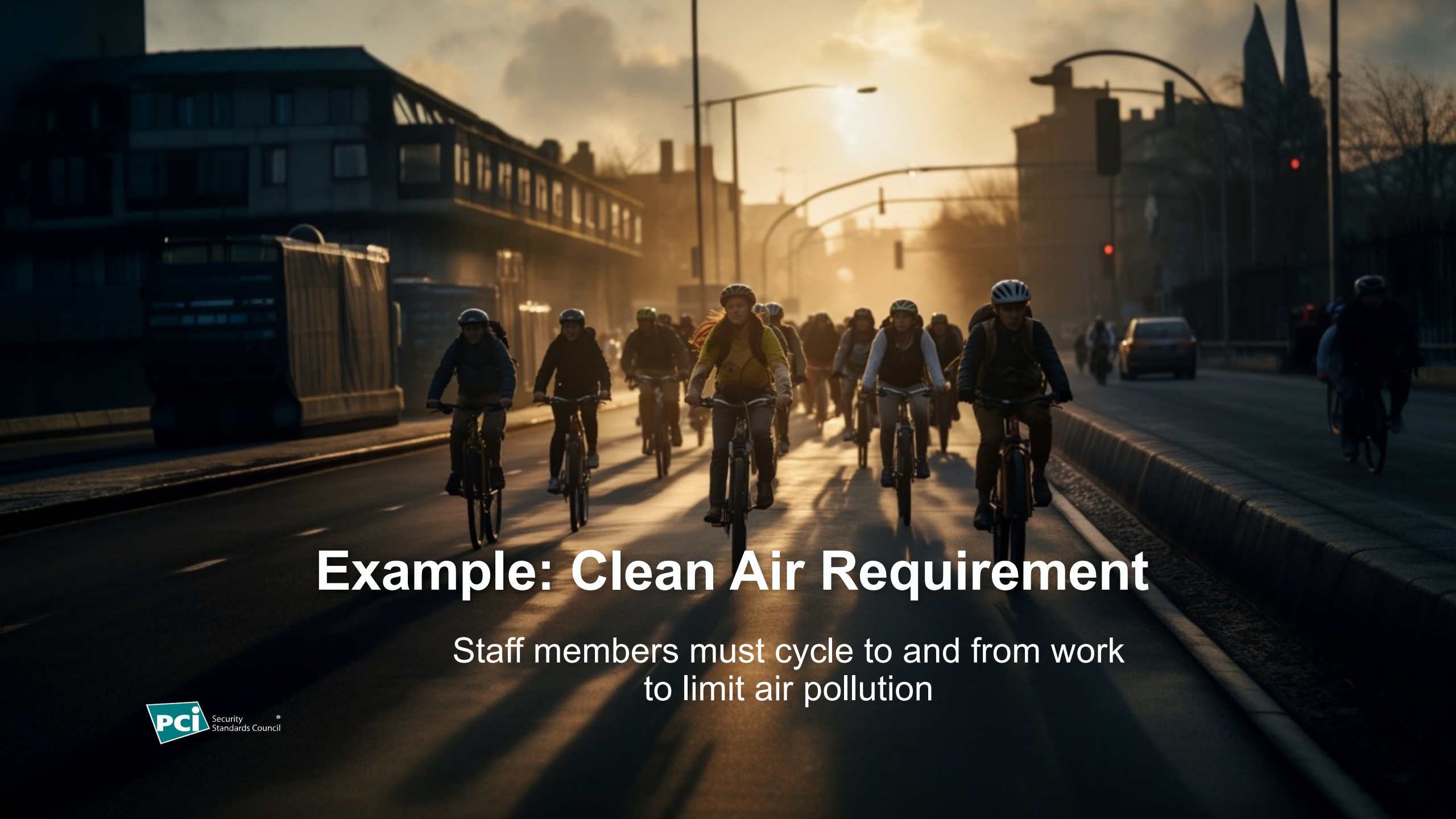
- Proactive
- Known business or technical constraint
- Cannot meet the requirement as stated
- Additional controls put in place to mitigate risk
- Typically documented by the entity being assessed

Business convenience to please 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

PCI Security Standards Council



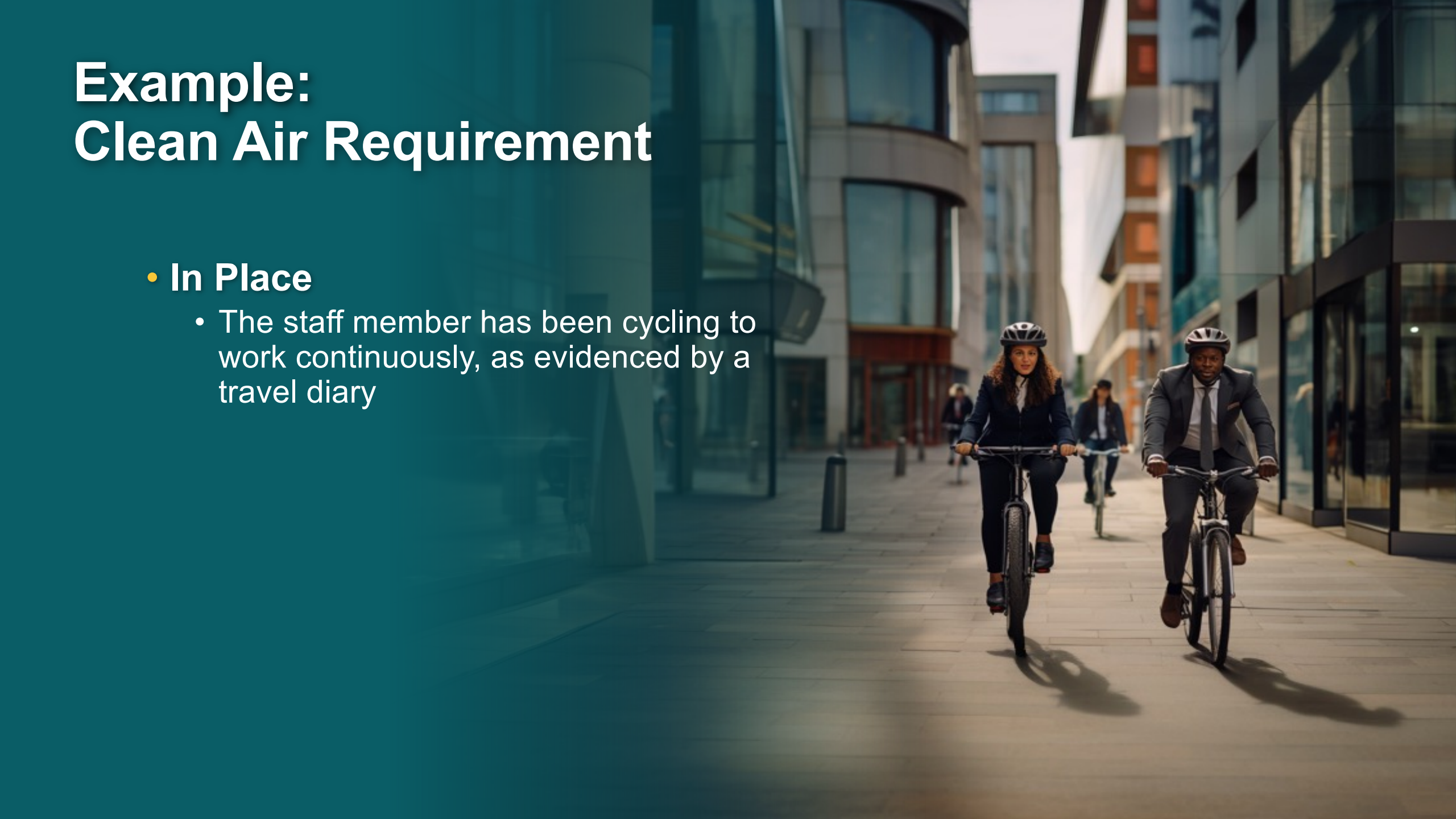
Example: Clean Air Requirement

Staff members must cycle to and from work
to limit air pollution

PCI Security Standards Council

Example:
Clean Air Requirement

- **In Place**
  - The staff member has been cycling to work continuously, as evidenced by a travel diary



Example:
Clean Air Requirement

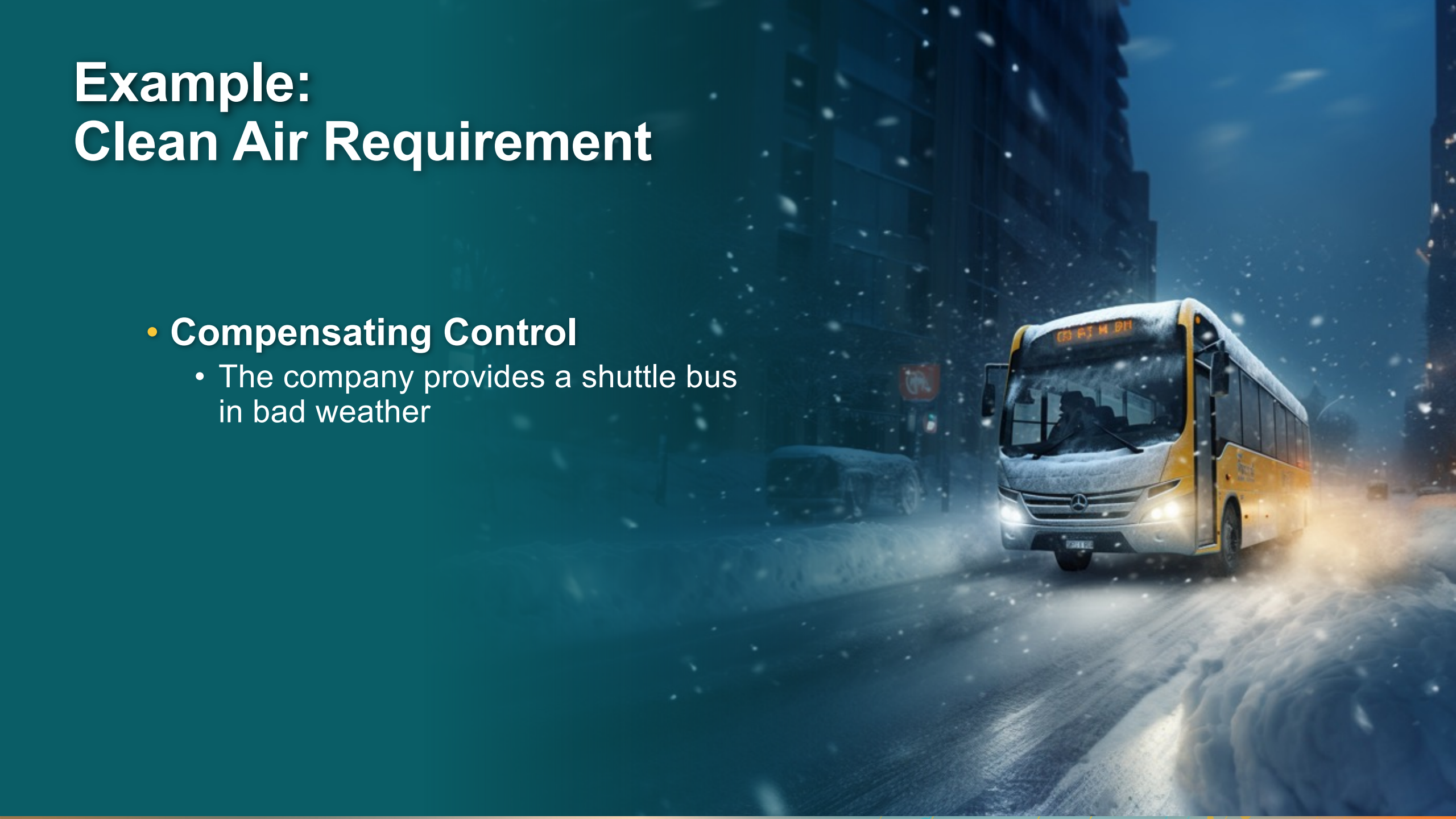
- **In Place**
  - The staff member has been cycling to work continuously, as evidenced by a travel diary

  - Item Noted For Improvement
    - Following a puncture, a staff member could not cycle to work
    - They used motorized transport for a few days until the puncture was fixed
    - Puncture repair kits were issued to all staff

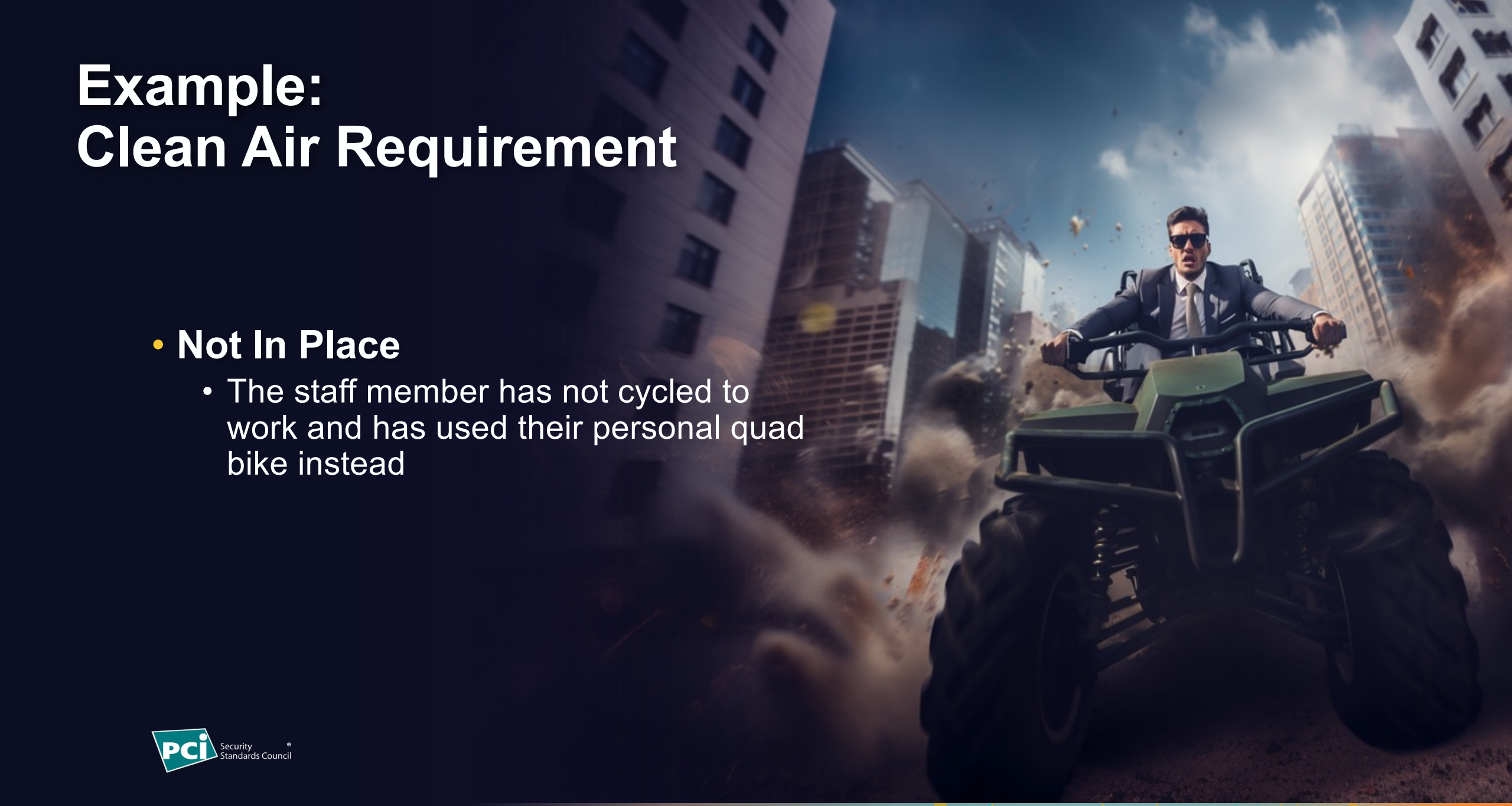
PCI Security Standards Council

Example:
Clean Air Requirement

- **Compensating Control**
  - The company provides a shuttle bus in bad weather



Example:
Clean Air Requirement



- **Not In Place**
  - The staff member has not cycled to work and has used their personal quad bike instead

PCI Security Standards Council


What if There Is a Legal Exception?
PCI
Security
Standards Council

What if There Is a Legal Exception?

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 *(Merchant Company Name)* 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.

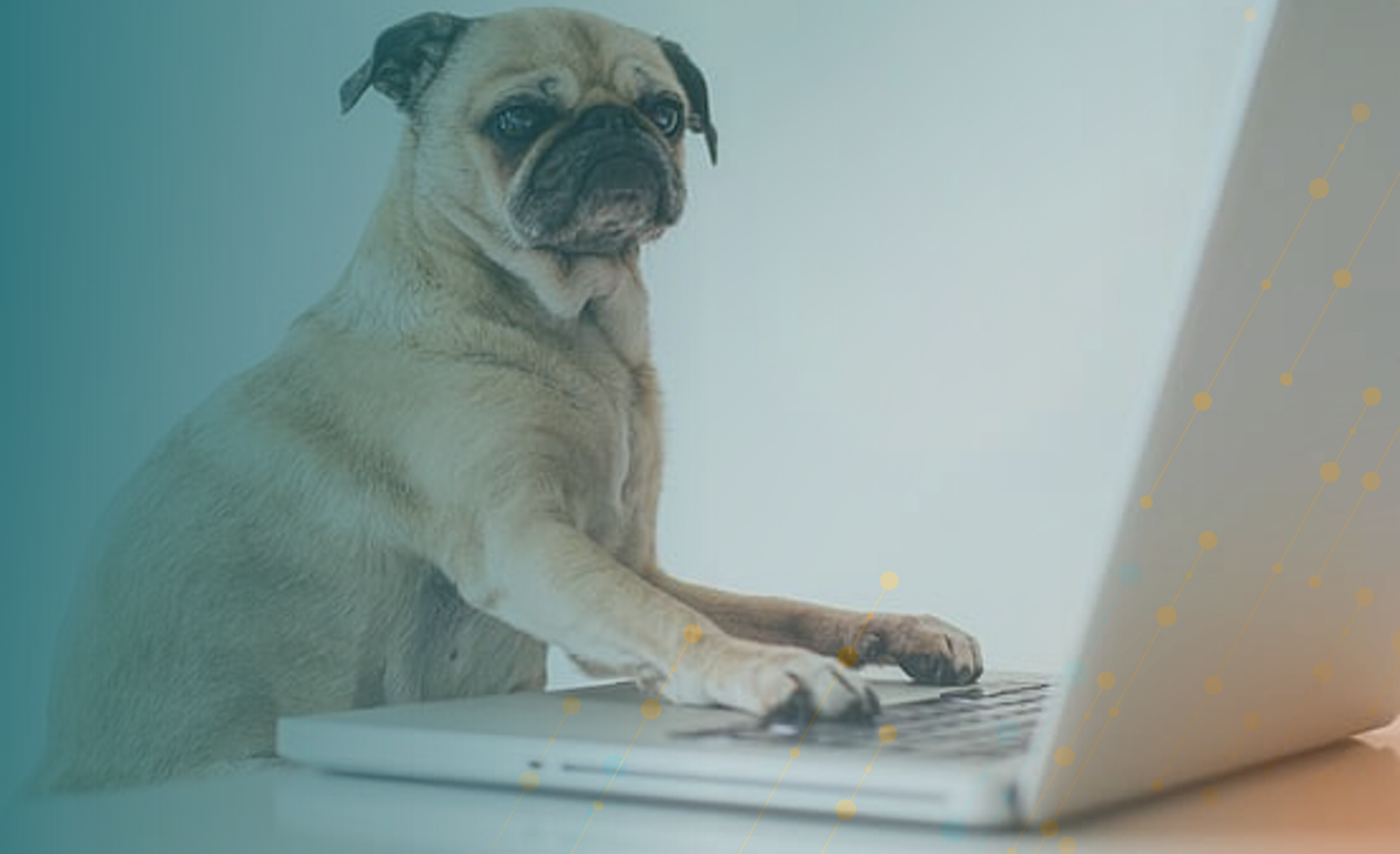
This option requires additional review from the entity to which this AOC will be submitted.

If selected, complete the following:

Affected Requirement	Details of how legal constraint prevents requirement from being met

PCI Security Standards Council

Example: PCI DSS Requirement



PCI DSS Requirement 11.3.2

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.

PCI Security Standards Council

Example: Requirement 11.3.2

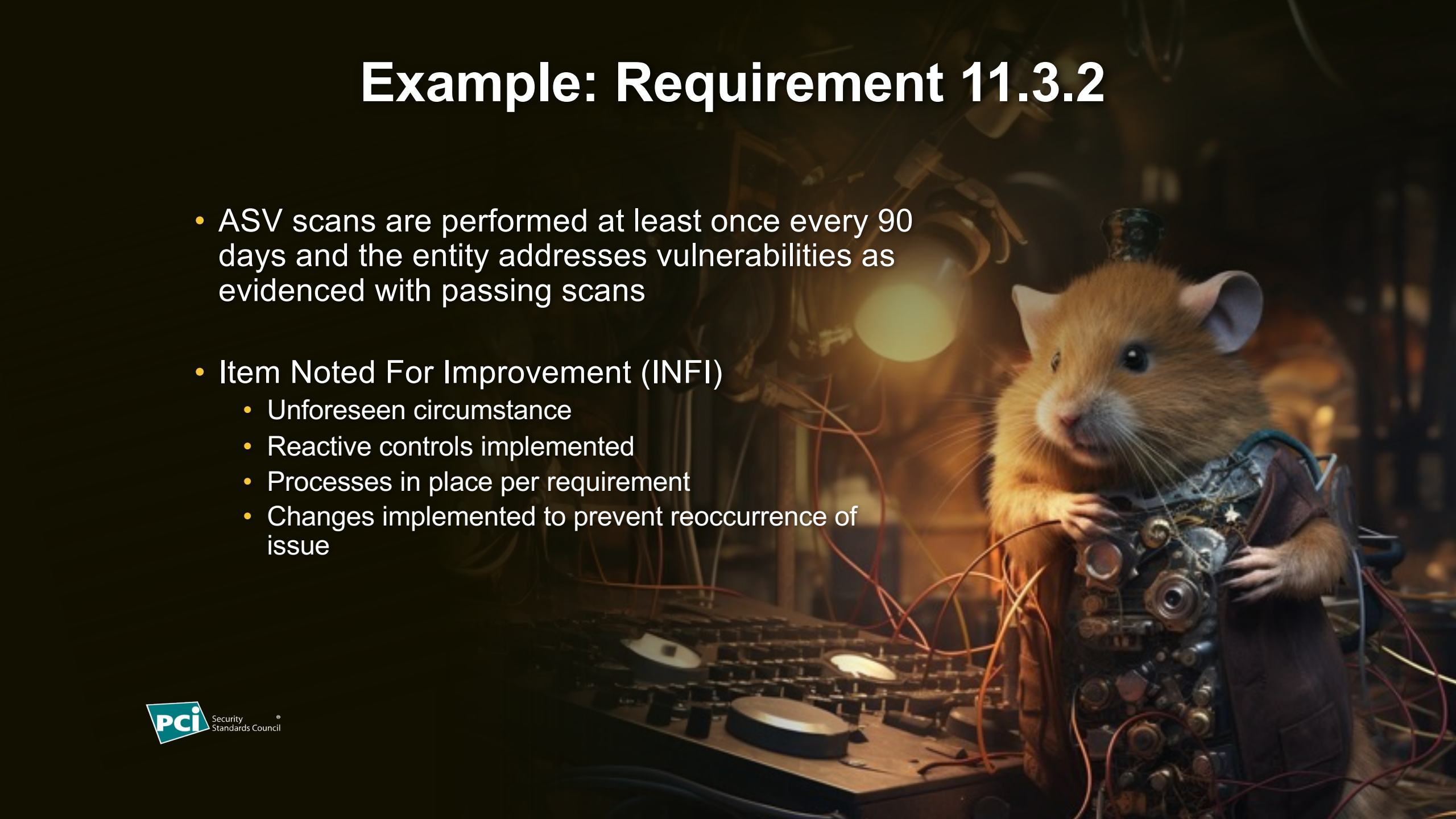
- ASV scans are performed at least once every 90 days and the entity addresses vulnerabilities as evidenced with passing scans

PCI Security Standards Council

Example: Requirement 11.3.2

- ASV scans are performed at least once every 90 days and the entity addresses vulnerabilities as evidenced with passing scans

- Item Noted For Improvement (INFI)
  - Unforeseen circumstance
  - Reactive controls implemented
  - Processes in place per requirement
  - Changes implemented to prevent reoccurrence of issue

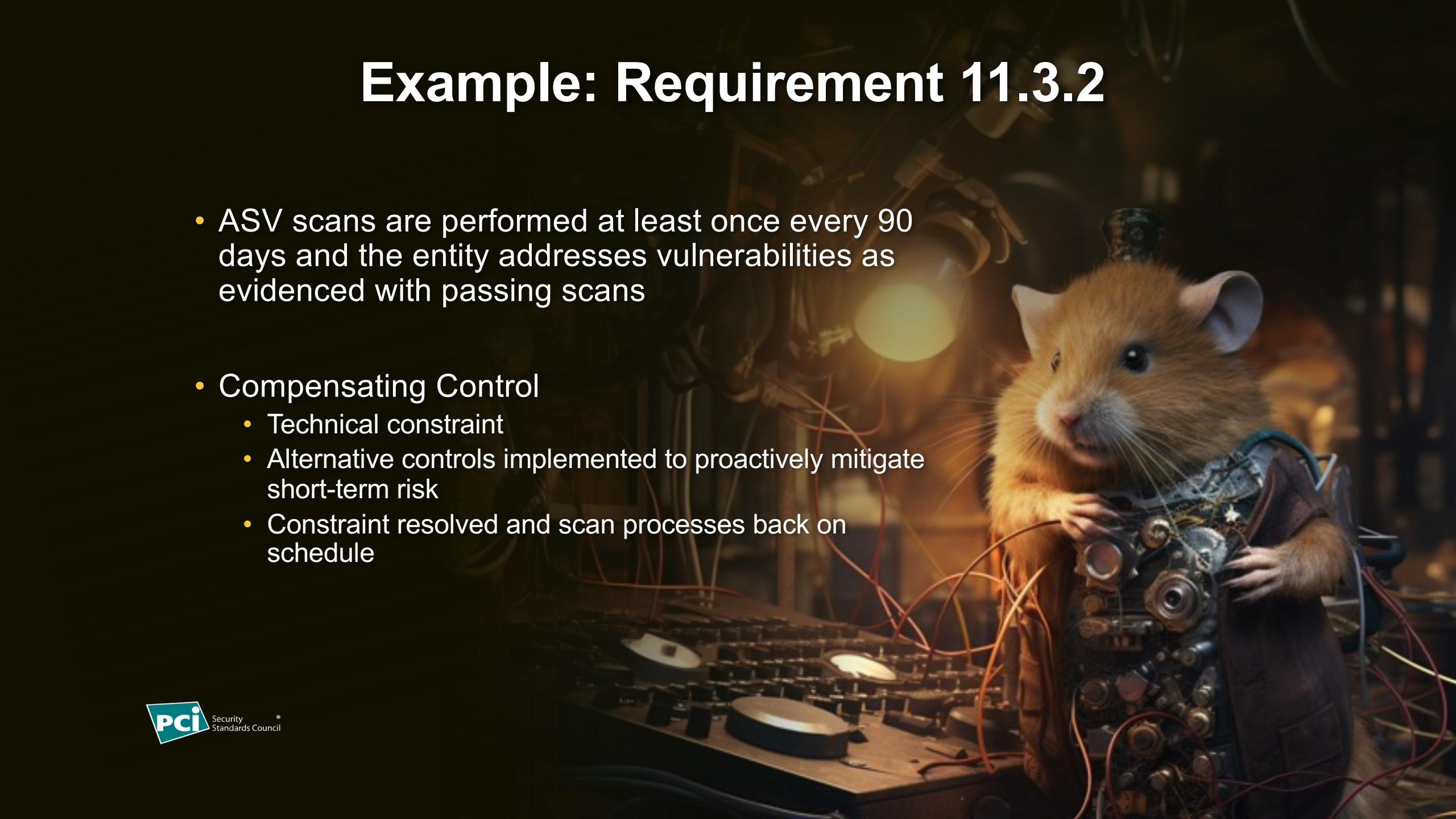


PCI Security Standards Council

Example: Requirement 11.3.2

- ASV scans are performed at least once every 90 days and the entity addresses vulnerabilities as evidenced with passing scans

- Compensating Control
  - Technical constraint
  - Alternative controls implemented to proactively mitigate short-term risk
  - Constraint resolved and scan processes back on schedule



PCI Security Standards Council

Frequently Asked Questions

- Template?

PCI Security Standards Council

Frequently Asked Questions

- Template?
- Assessors?

PCI Security Standards Council

Frequently Asked Questions

- Template?
- Assessors?
- Assessment types?

PCI Security Standards Council

Frequently Asked Questions

- Template?
- Assessors?
- Assessment types?
- Signatures?

PCI Security Standards Council

Frequently Asked Questions

- Template?
- Assessors?
- Assessment types?
- Signatures?
- PCI DSS version?

PCI Security Standards Council

Frequently Asked Questions

- Template?
- Assessors?
- Assessment types?
- Signatures?
- PCI DSS version?
- Resources?

PCI Security Standards Council

All About INFI

PCI Security Standards Council

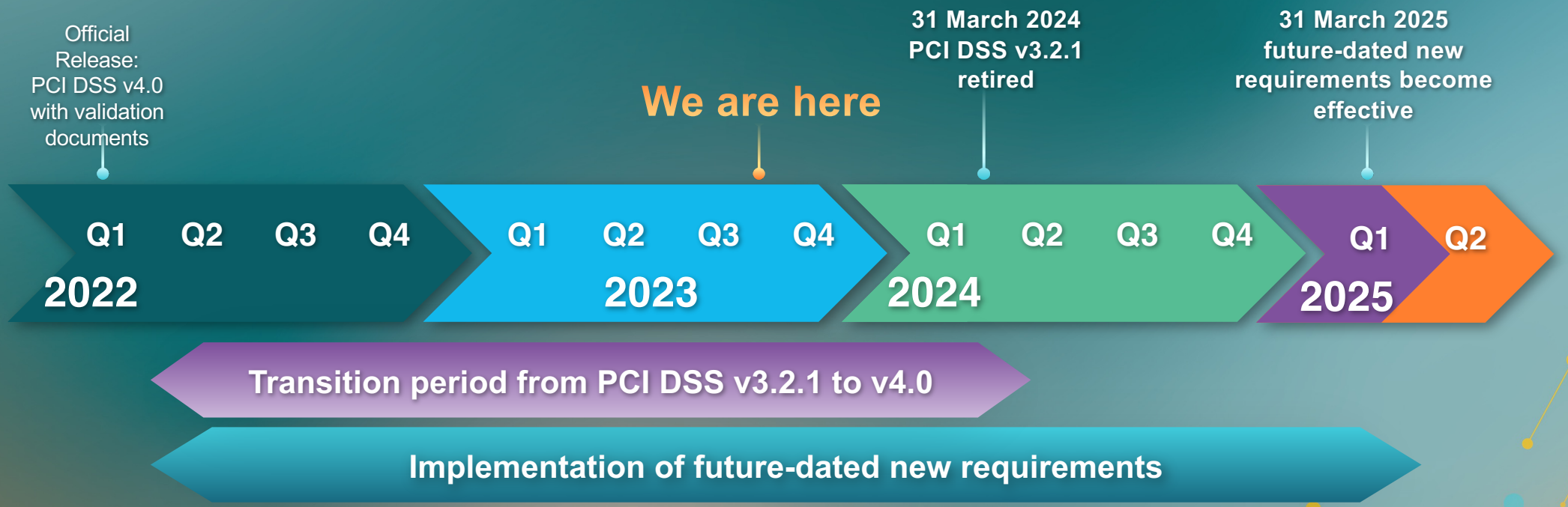
PCI Security Standards Council

What To Do Next?

PCI DSS v4.0 - Part 3


PCI
Security
Standards Council

PCI DSS v4.0 Implementation Timeline



PCI Security Standards Council

New Requirements

53

New requirements that apply to all entities

11

Additional requirements for service providers

13

Effective immediately for all v4.0 assessments

PCI Security Standards Council

Will the Dates for PCI DSS v4.0 Change?

NO

PCI Security Standards Council

Steps on Your PCI DSS v4.0 Journey

pcissc.org/ eight-steps-to-take-toward-pci-dss-v4-0

#1 Start Now

PCI Security Standards Council

#2 Stay Strong

PCI Security Standards Council

#3

Understand The Requirements

PCI Security Standards Council

#4 Understand Validation Options

PCI Security Standards Council


#5
Do The Work
PCI
Security
Standards Council

#6

Use Trusted Partners

PCI Security Standards Council

#7

Do Your Own Assessments

PCI Security Standards Council

#8

Prioritize Security As A Continuous Process

PCI Security Standards Council

Let’s Answer Some Stakeholder Questions!

PCI Security Standards Council

Do the deadlines apply to the start or end date of an assessment?

PCI Security Standards Council

What should an entity do if its v3.2.1 assessment will not be complete prior to the standard's retirement date?

FAQ 1563

- PCI DSS v3.2.1 is retiring on 31 March 2024
- PCI SSC will not be updating or supporting v3.2.1 after that date
- But what if your v3.2.1 assessment will not be done by then?
- Ask your acquirer or the payment brands

PCI Security Standards Council

Do assessment results expire on 31 March 2024 or are they valid for a year?

PCI Security Standards Council

Does an entity's PCI DSS assessment result expire when the standard is retired?

FAQ 1565

- How long an assessment result is valid does not change when the standard is retired
- Questions? Ask your acquirer or the payment brands

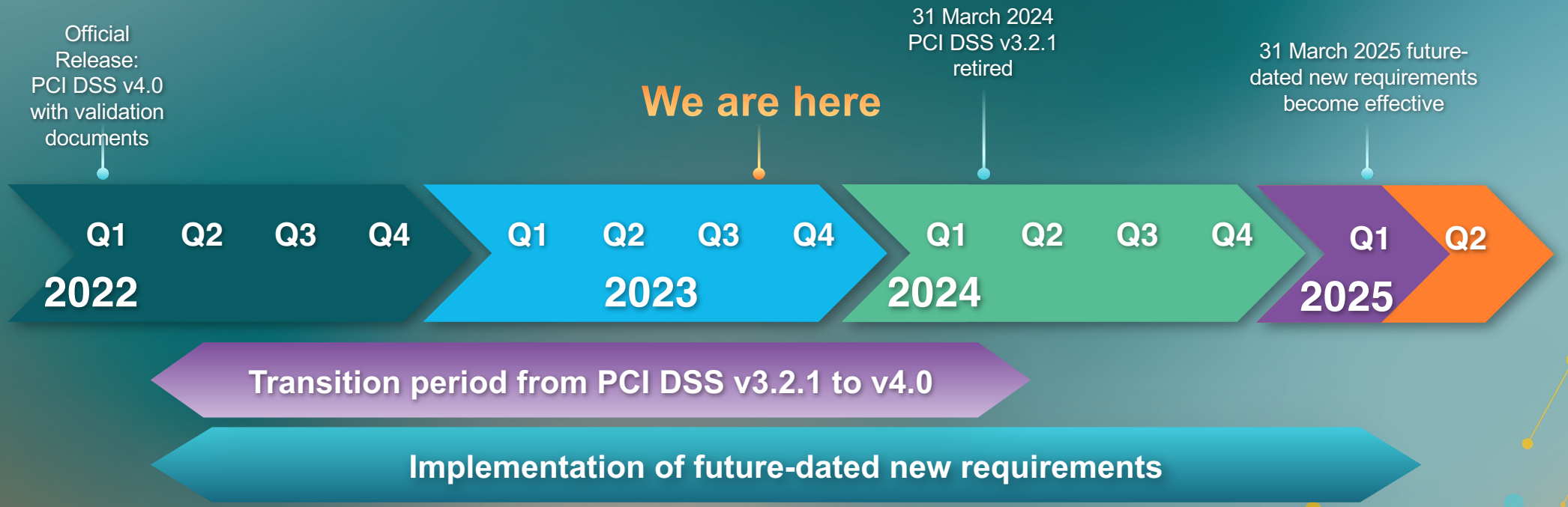
PCI Security Standards Council

The two dates are confusing:
31 March 2024
31 March 2025

What do those different dates mean?

PCI Security Standards Council

PCI DSS v4.0 Implementation Timeline



PCI Security Standards Council

Do SAQ A merchants need four passing ASV scans before they can submit their v4.0 assessment results?

PCI Security Standards Council

What is the meaning of “initial PCI DSS assessment”?

FAQ 1485

- Initial assessment applies when an entity is assessed to a requirement for the first time
- Merchants do not need four passing scans for their initial assessment to this requirement

PCI Security Standards Council

Does a TPSP need to be assessed to v4.0 before their customers move to v4.0?

PCI Security Standards Council

Can an entity be PCI DSS compliant if they use a third-party service provider (TPSP) that is validated to a previous version of PCI DSS?

FAQ 1282

- Entities can be compliant with v4.0 using TPSPs validated to v3.2.1
- If TPSP's v3.2.1 validation was completed prior to 31 March 2024
- If TPSP's validation is still current
- Questions? Ask your acquirer or the payment brands

PCI Security Standards Council


PCI DSS v4.0
Limited Revision
PCI
Security
Standards Council

PCI DSS v4.0 Resources

pcissc.org/resourcehub

PCI Security Standards Council


PCI
Security
Standards Council
Thank You!