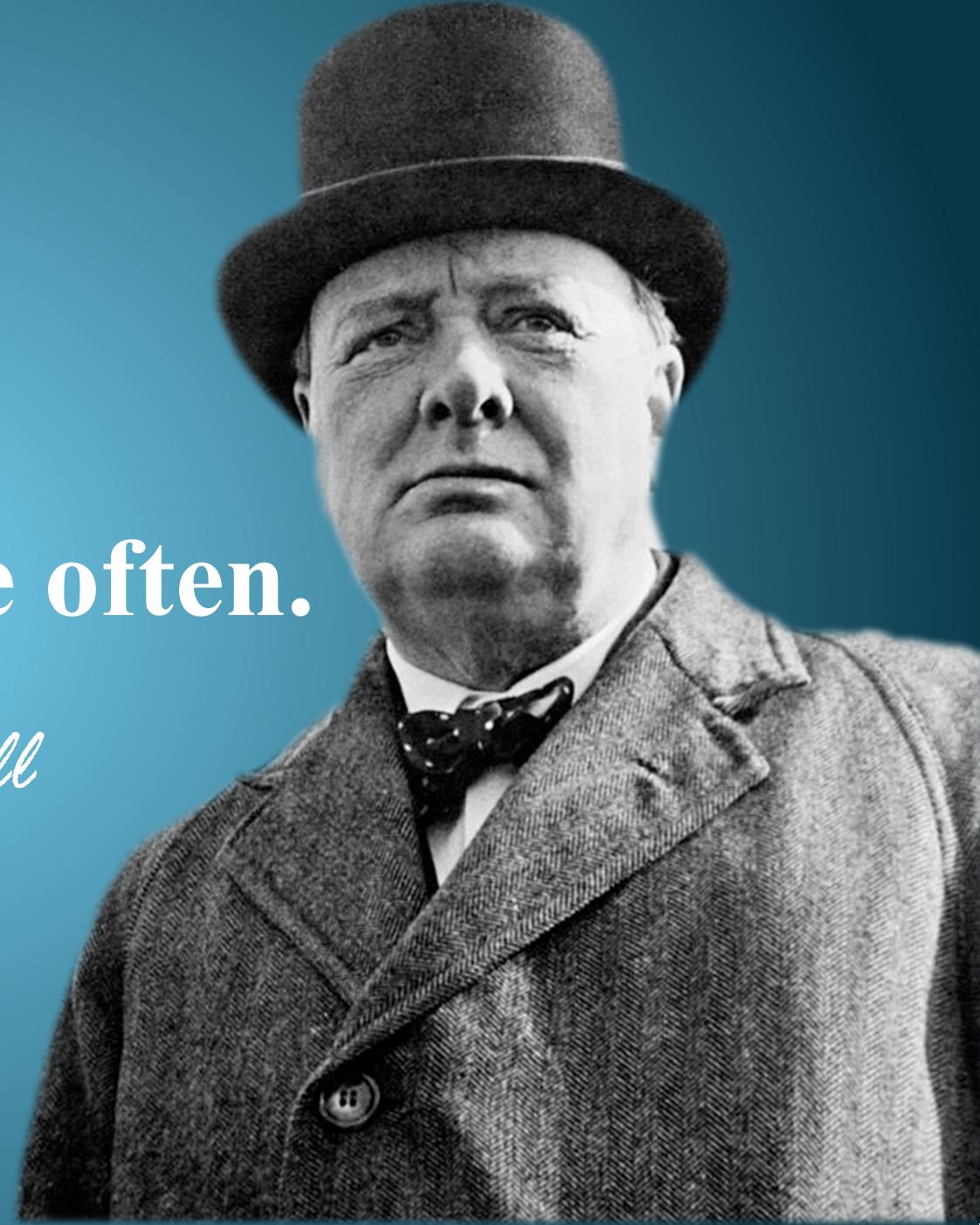


To improve is to change;  
to be perfect is to change often.

*Winston Churchill*



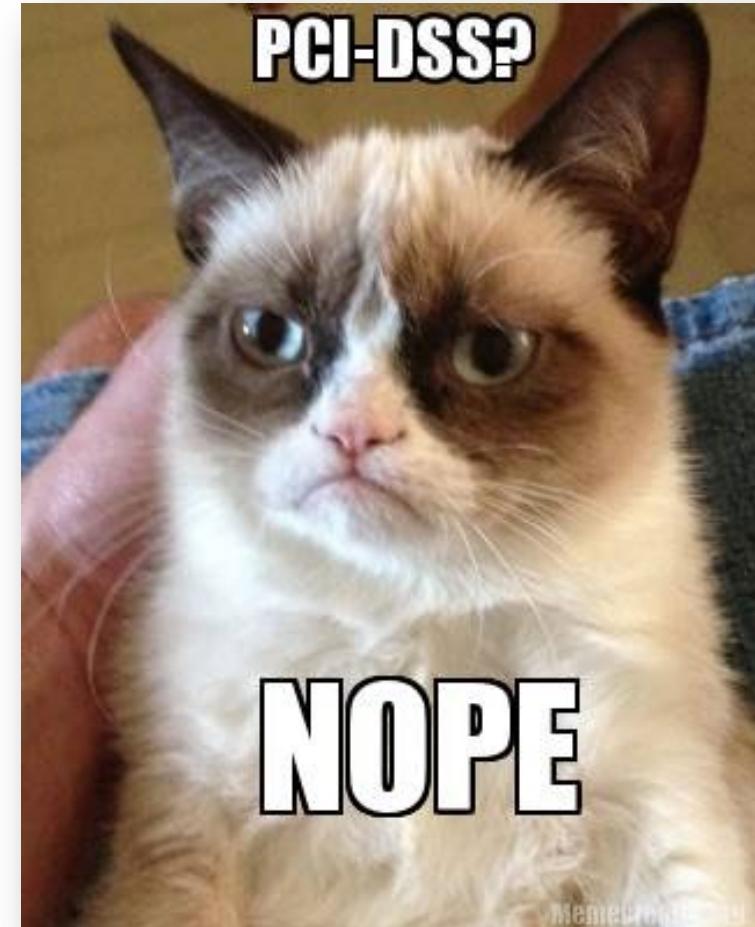


# PCI DSS v4.0 Is Here – Now What?

SEPTEMBER 2023

[LBMC.COM](http://LBMC.COM)

# New Standard, Who Dis?



# About Me

**KYLE HINTERBERG, QSA, CISSP, CISA, AWS SCS  
MANAGER, LBMC**

I AM A QSA, BUT I AM NOT YOUR QSA

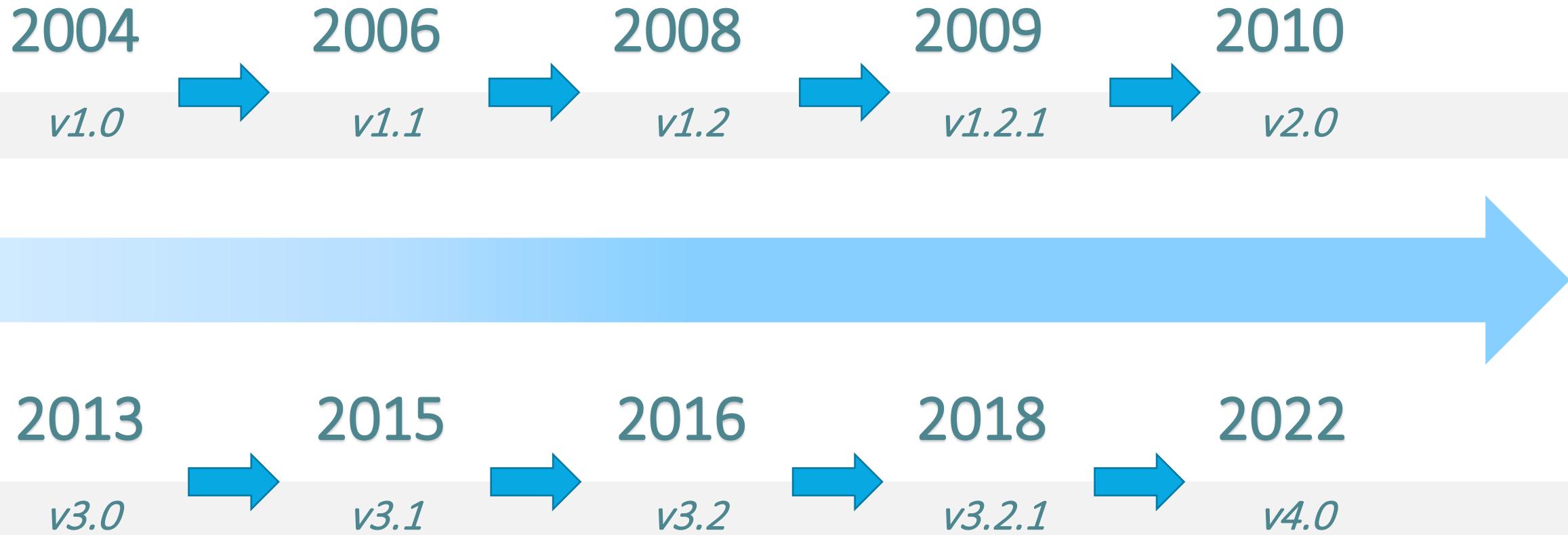
- [kyle.hinterberg@lbmc.com](mailto:kyle.hinterberg@lbmc.com)
- [linkedin.com/in/kylehinterberg](https://linkedin.com/in/kylehinterberg)



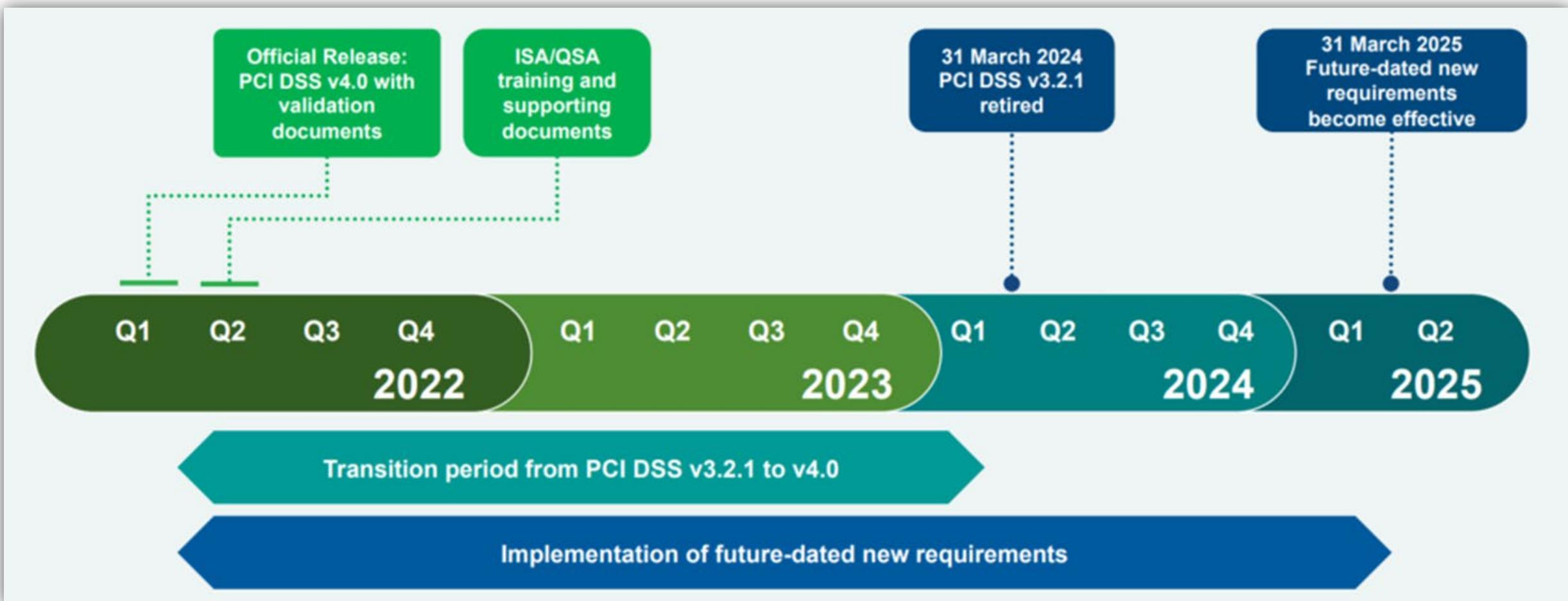
# The Payment Card Industry



# PCI DSS Releases



# PCI DSS v4.0 Schedule



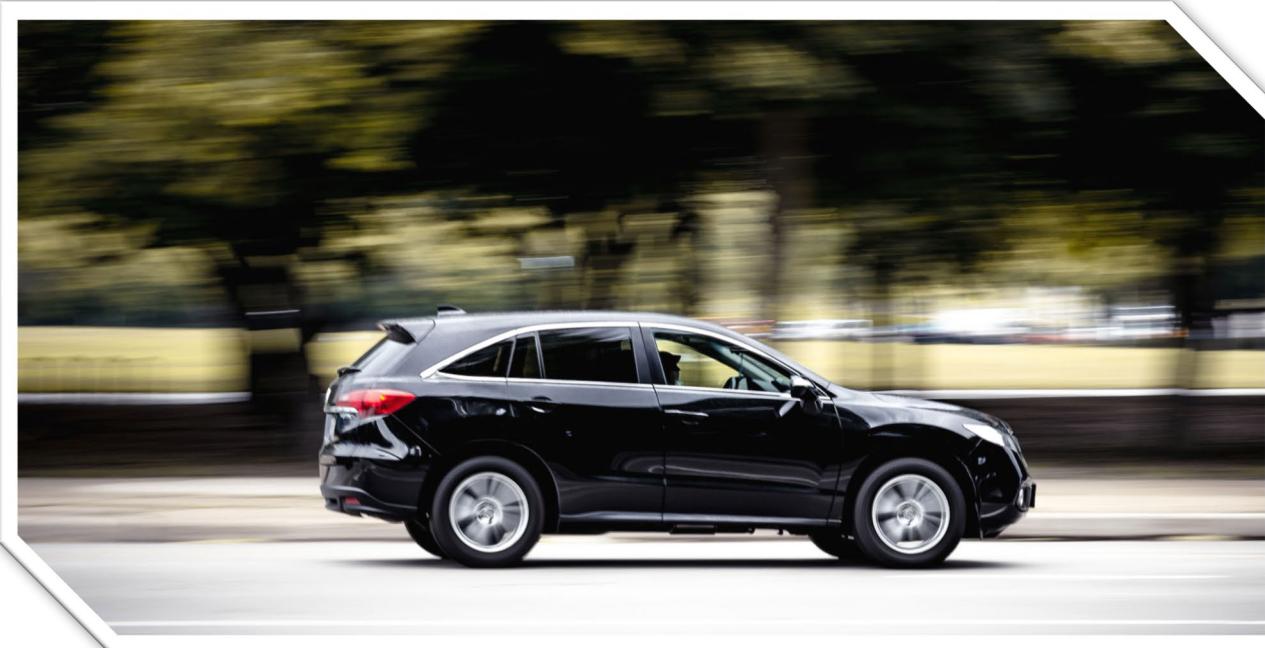
<https://blog.pcisecuritystandards.org/at-a-glance-pci-dss-v4-0>

# What's New?

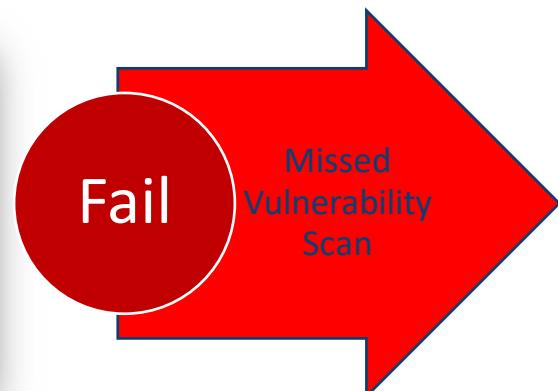
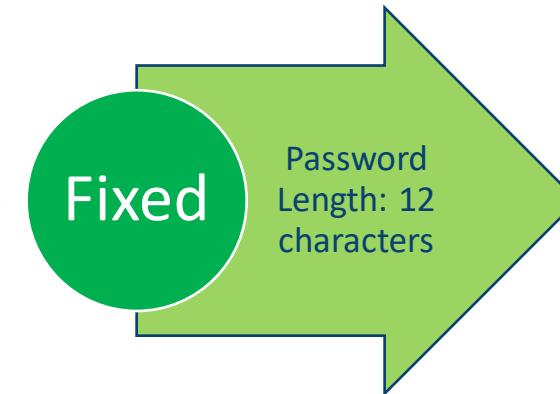
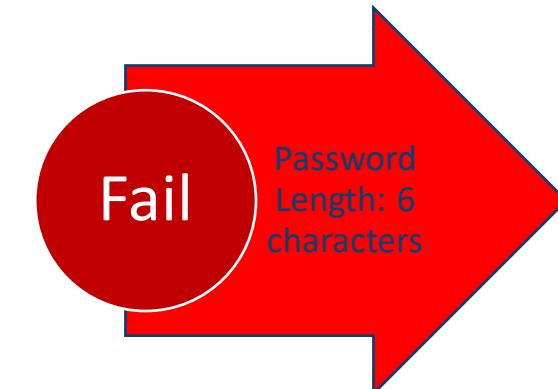


# Defined Approach vs Customized Approach

## Objective: Get to Work



# Items Noted For Improvement (INFI) Worksheet



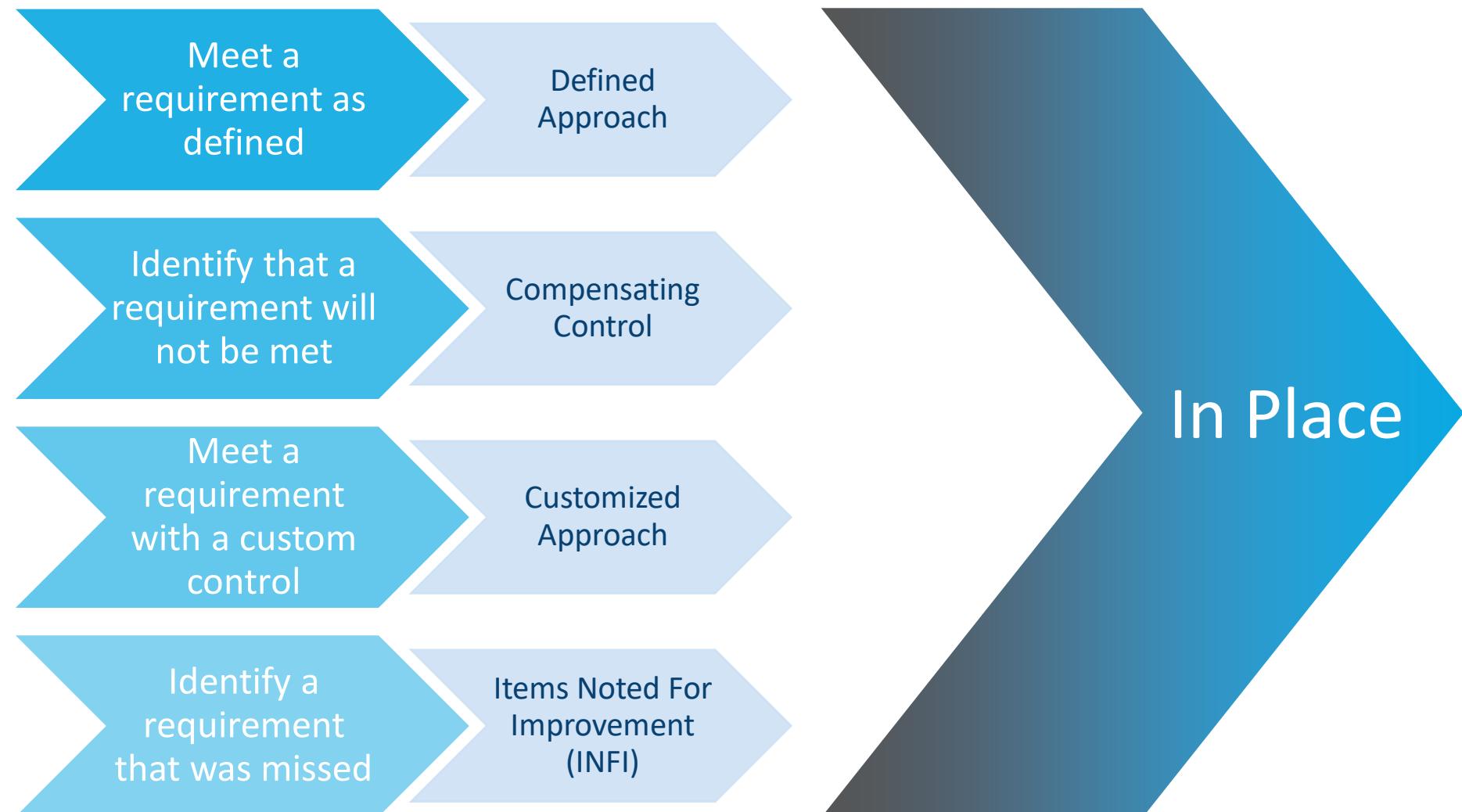
# Items Noted For Improvement (INFI) Worksheet

- 1 • Repeatable, documented process
- 2 • Missed due to an exceptional circumstance
- 3 • Root cause has been addressed
- 4 • Process updated to prevent recurrence



In Place

# Flexible Compliance



# 64 New Requirements

## Applicability

**53**  
All Entities

**11**  
Service  
Providers

## Effective Date

**13**  
Immediately  
for all v4.0  
assessments

**51**  
April 1, 2025

# Roles & Responsibilities

- Roles and responsibilities for performing activities are:
  - Documented
  - Assigned
  - Understood



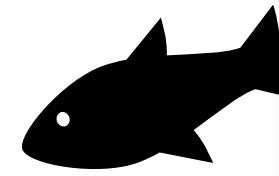
# Account Data Storage and Encryption

- Bank Identification Number (BIN) and last four digits
- Sensitive Authentication Data (SAD)



# Phishing Protection

- Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks



# Payment Page Security

- All payment page scripts are:
  - Authorized
  - Inventoried
  - Justified
  - And their integrity is confirmed
- Detection of unauthorized modifications to the HTTP headers and the contents of payment pages

The screenshot shows a payment page for GrrCON 2023. At the top, it says "GrrCON 2023" and "September 28 · 8am - September 29 · 6pm EDT". On the right, there is a logo for "GrrCON" featuring a green skull.

The page lists two ticket types:

- Early Bird**: \$90.00 + \$7.88 Fee. Quantity: 0. Status: Sold out. Note: Limited number of early tickets. A "See more" link is present.
- VIP**: \$350.00 + \$25.32 Fee. Quantity: 0. Status: Sold out. Description: Regular ticket plus: Access to Presentation Sessions w/ Priority VIP only table seating (many with electric) - VIP/Speaker Lounge Access (You want this) - Access to FREE workshops (separate See more link).

At the bottom, there is a red warning message: "Add at least 1 ticket" and a large orange "Check out" button.

# User Account Controls

- Passwords need to be at least 12 characters long
- Shared accounts can be used on an exception basis
- Passwords do not need to be rotated if one of the following is met:
  1. Multifactor authentication (MFA)
  2. The security posture of accounts is dynamically analyzed
- MFA is implemented to secure access into the cardholder data environment (CDE).



# System Account Controls

- Accounts are assigned via the principle of least privilege
- Accounts that can be used for interactive login are appropriately managed
- Passwords are changed periodically or upon suspicion/confirmation of compromise



# Penetration Testing

- Penetration test findings need to be corrected in accordance with an entity's assessment of the risk posed by the security issue



# Log Reviews & Alerts

- Automated mechanisms are used to perform audit log reviews
- Failures of critical security control systems are:
  - Detected
  - Alerted
  - Addressed promptly



# Internal Vulnerability Scans

- Internal vulnerability scans are performed via authenticated scanning.

Driving back home after printing out the vulnerability scan report

| Timeframes in PCI DSS Requirements | Descriptions and Examples  |
|------------------------------------|--|
| Daily                              | Every day of the year (not only on business days).   |
| Weekly                             | At least once every seven days.  |
| Monthly                            | At least once every 30 to 31 days, or on the n <sup>th</sup> day of the month.   |
| Every three months ("quarterly")   | At least once every 90 to 92 days, or on the n <sup>th</sup> day of each third month.  |
| Every six months                   | At least once every 180 to 184 days, or on the n <sup>th</sup> day of each sixth month.  |
| Every 12 months ("annually")       | At least once every 365 (or 366 for leap years) days or on the same date every year.   |
| Periodically                       | Frequency of occurrence is at the entity's discretion and is documented and supported by the entity's risk analysis. The entity must demonstrate that the frequency is appropriate for the activity to be effective and to meet the intent of the requirement. |
| Immediately                        | Without delay. In real time or near real time.   |
| Promptly                           | As soon as reasonably possible.  |



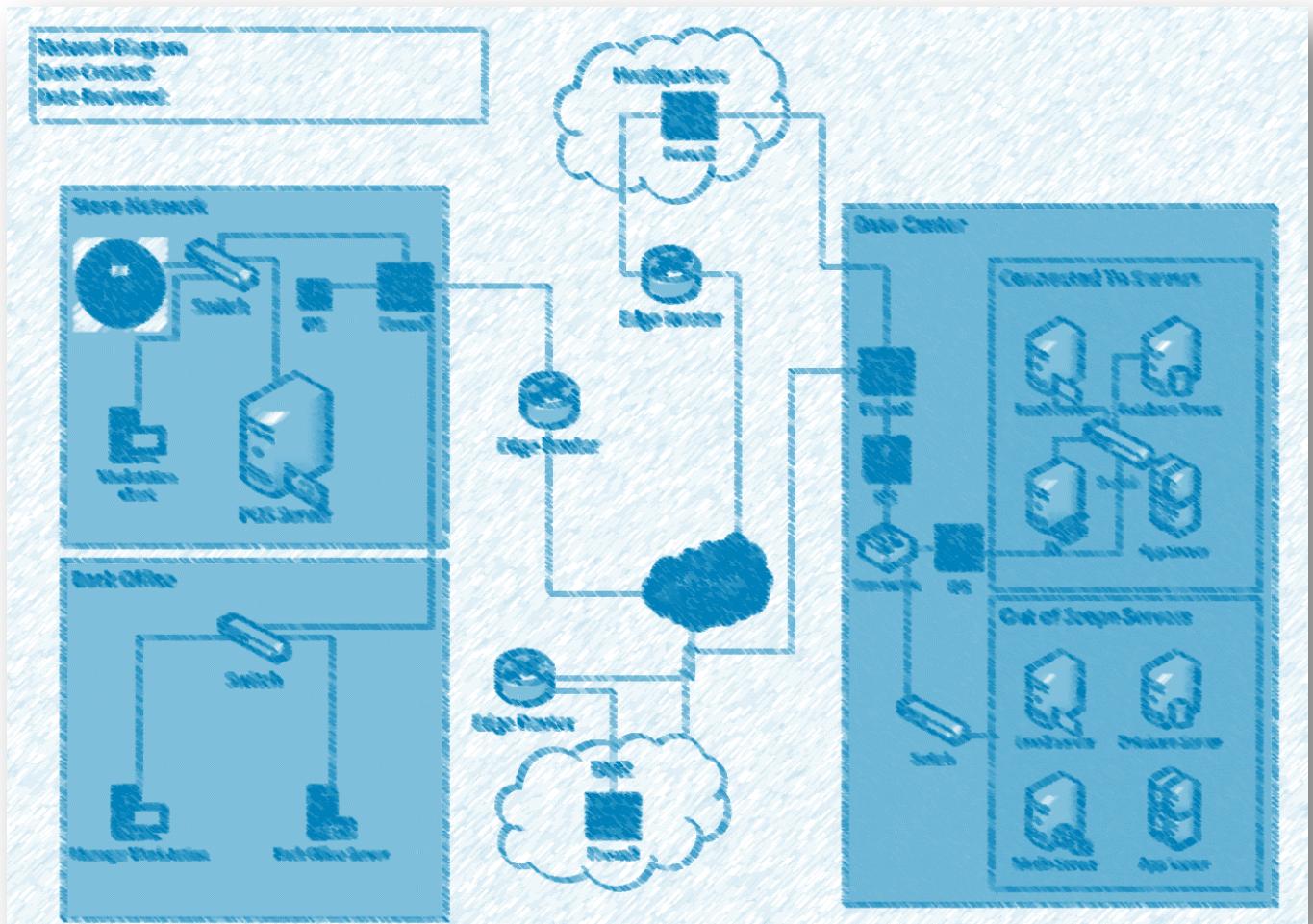
# Risk Assessments

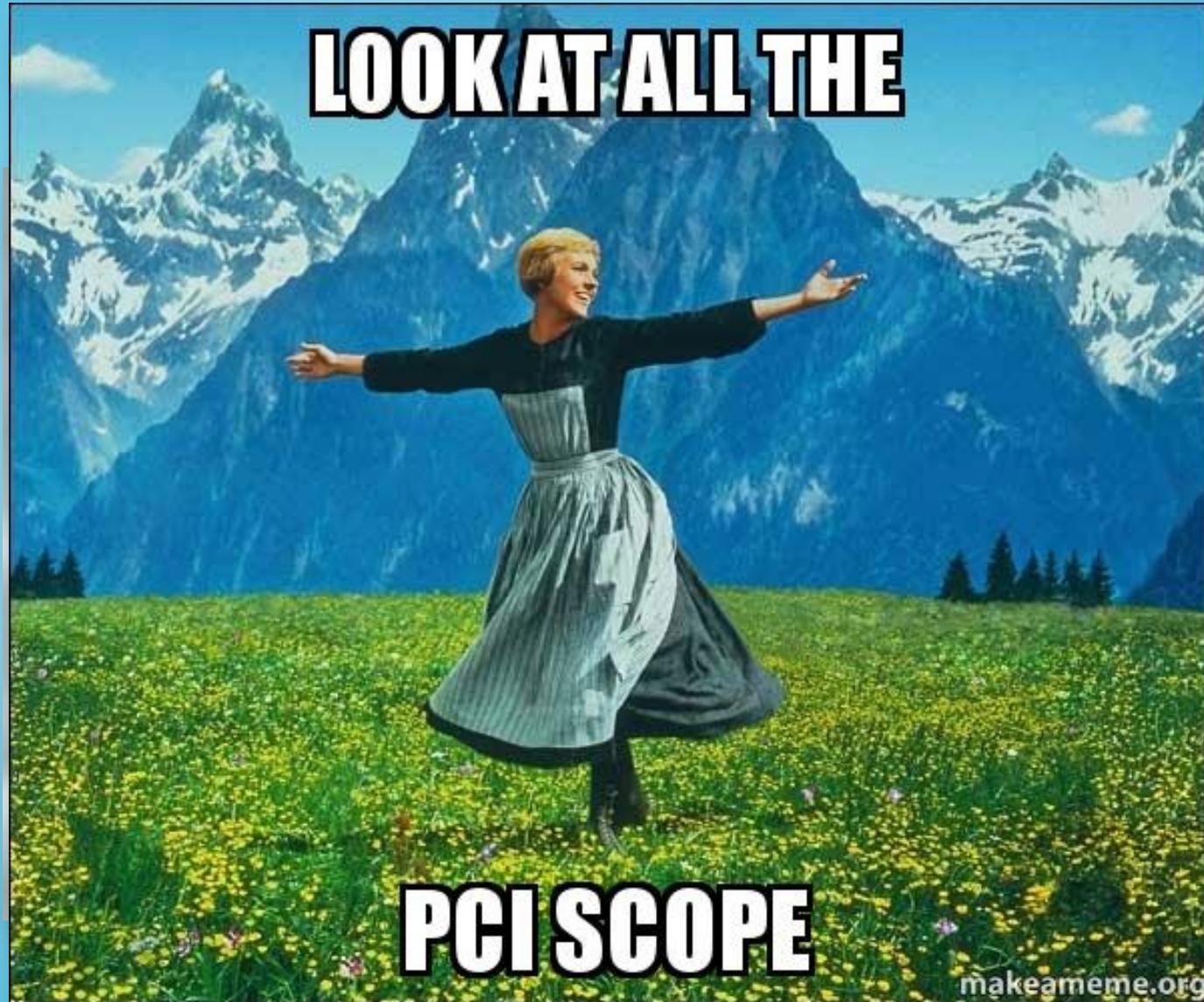
- Enterprise risk assessments are no longer required
- Targeted Risk Analyses (TRAs)
  1. TRAs for use with a Customized Approach
  2. TRAs for requirements which allow for flexibility



# Environment Reviews

- PCI DSS scope is documented and validated
- Reviews and Inventories:
  - Keys and certificates
  - Hardware and software
  - User and system accounts
  - Cryptographic cipher suites and protocols





# ANY QUESTIONS?



**Kyle Hinterberg, QSA, CISSP, CISA, AWS SCS  
Manager, LBMC**

[kyle.hinterberg@lbmc.com](mailto:kyle.hinterberg@lbmc.com)  
[linkedin.com/in/kylehinterberg](https://linkedin.com/in/kylehinterberg)



To improve is to change;  
to be perfect is to change often.

[www.LBMC.com](http://www.LBMC.com)