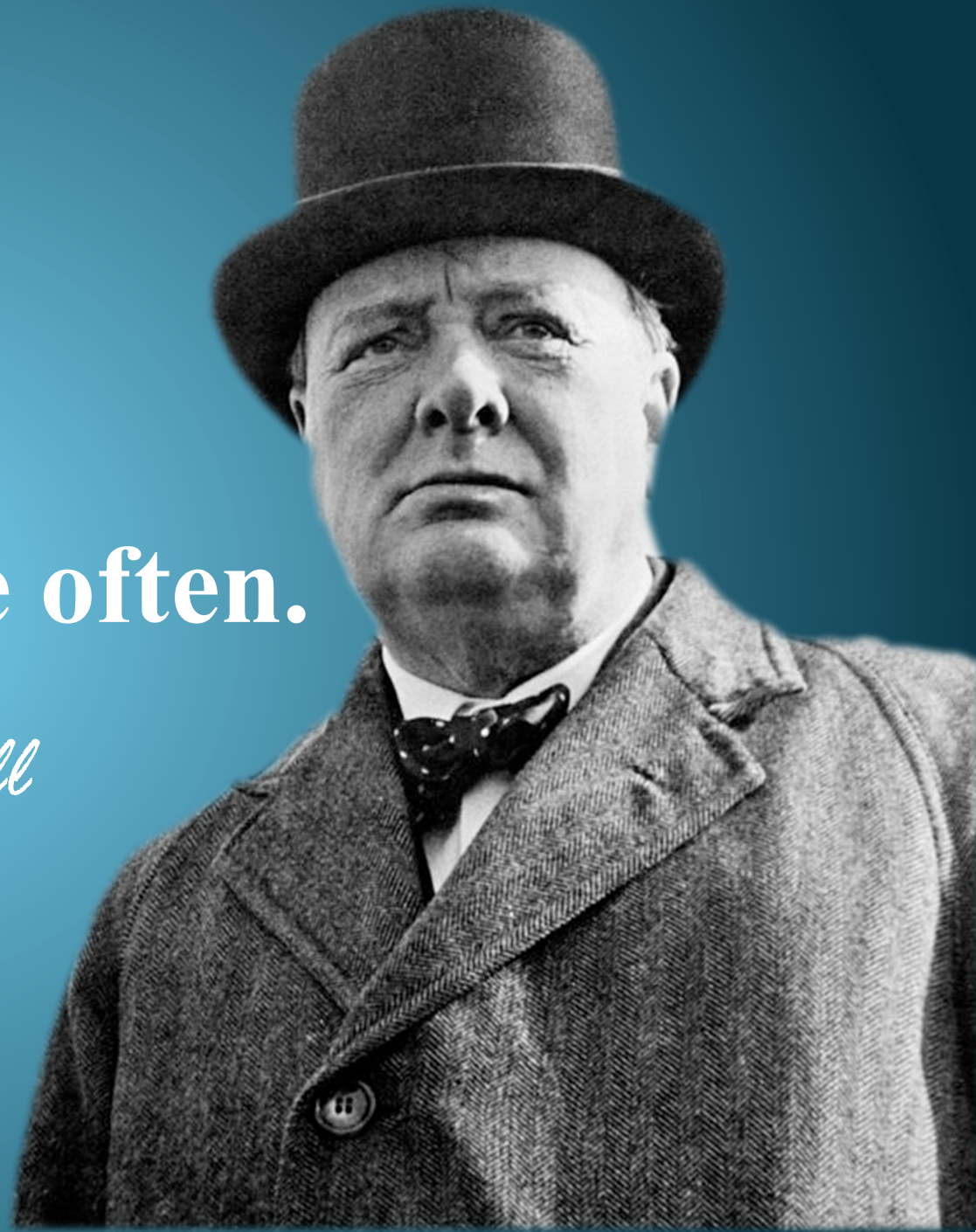
To improve is to change;
to be perfect is to change often.

Winston Churchill



LBMC

PCI DSS v4.0 Is Here – Now What?

AUGUST 2023

LBMC.COM

New Standard, Who Dis?

About Me

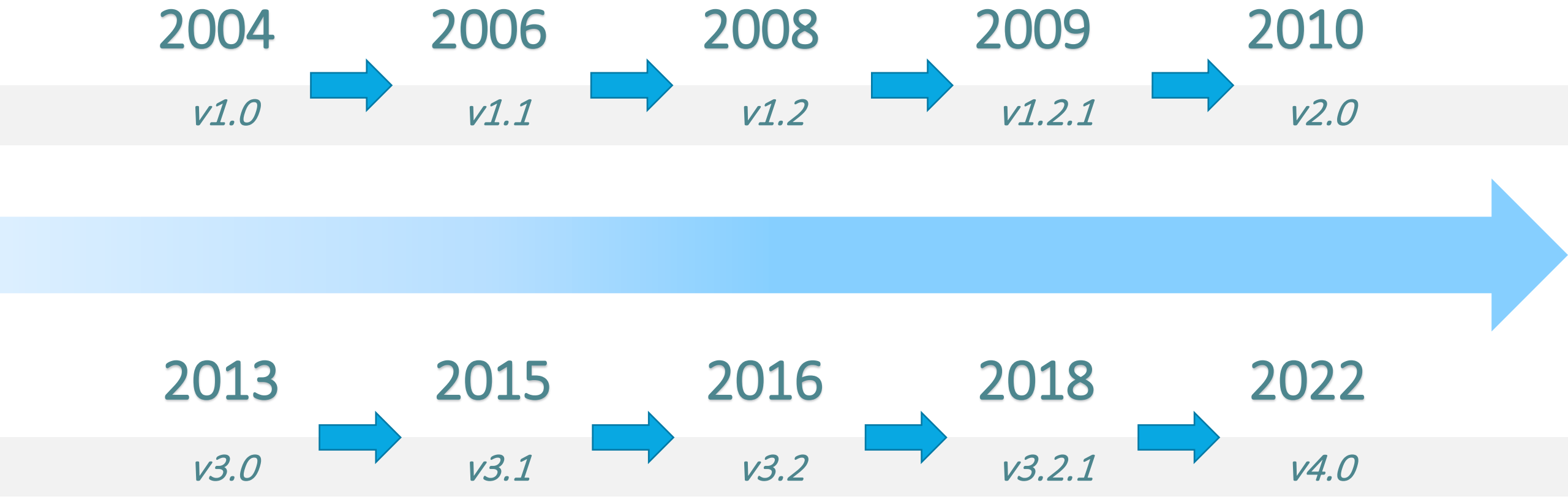
KYLE HINTERBERG, *QSA, CISSP, CISA, AWS SCS*
MANAGER, LBMC

I AM A QSA, BUT I AM NOT **YOUR** QSA

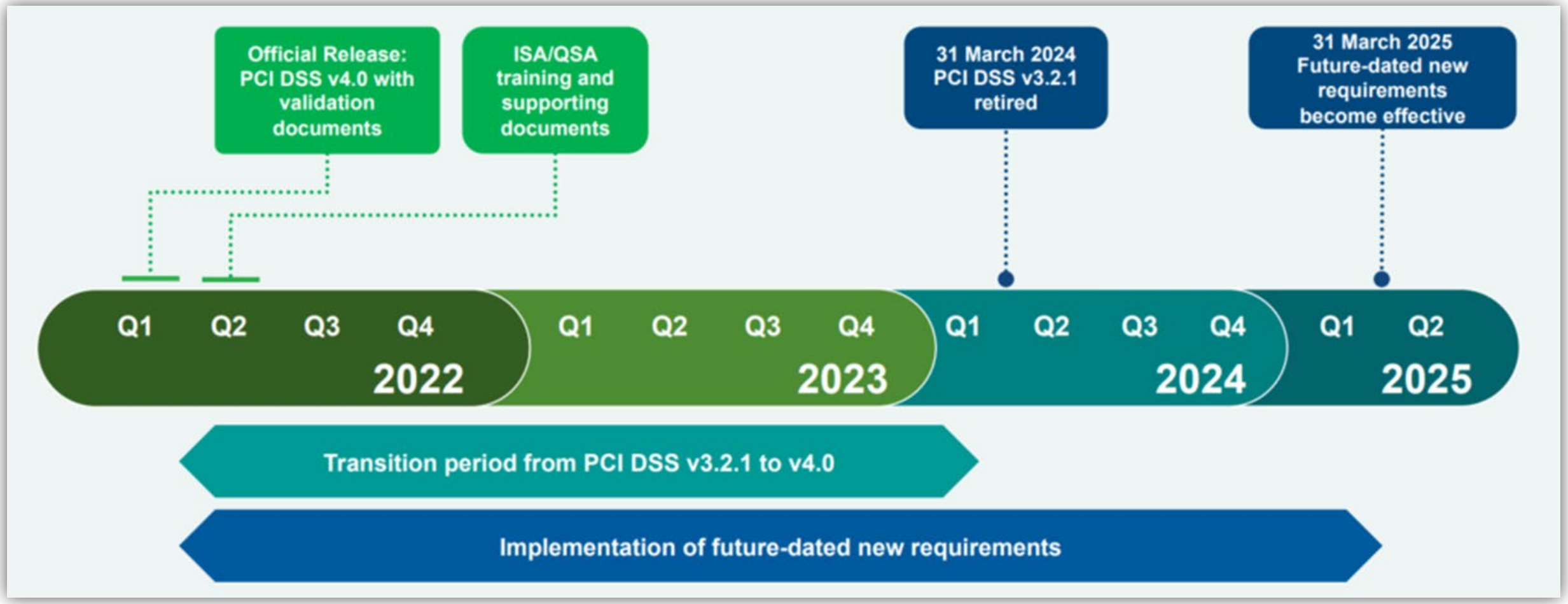
- kyle.hinterberg@lbmc.com
- linkedin.com/in/kylehinterberg

The Payment Card Industry

PCI DSS Releases

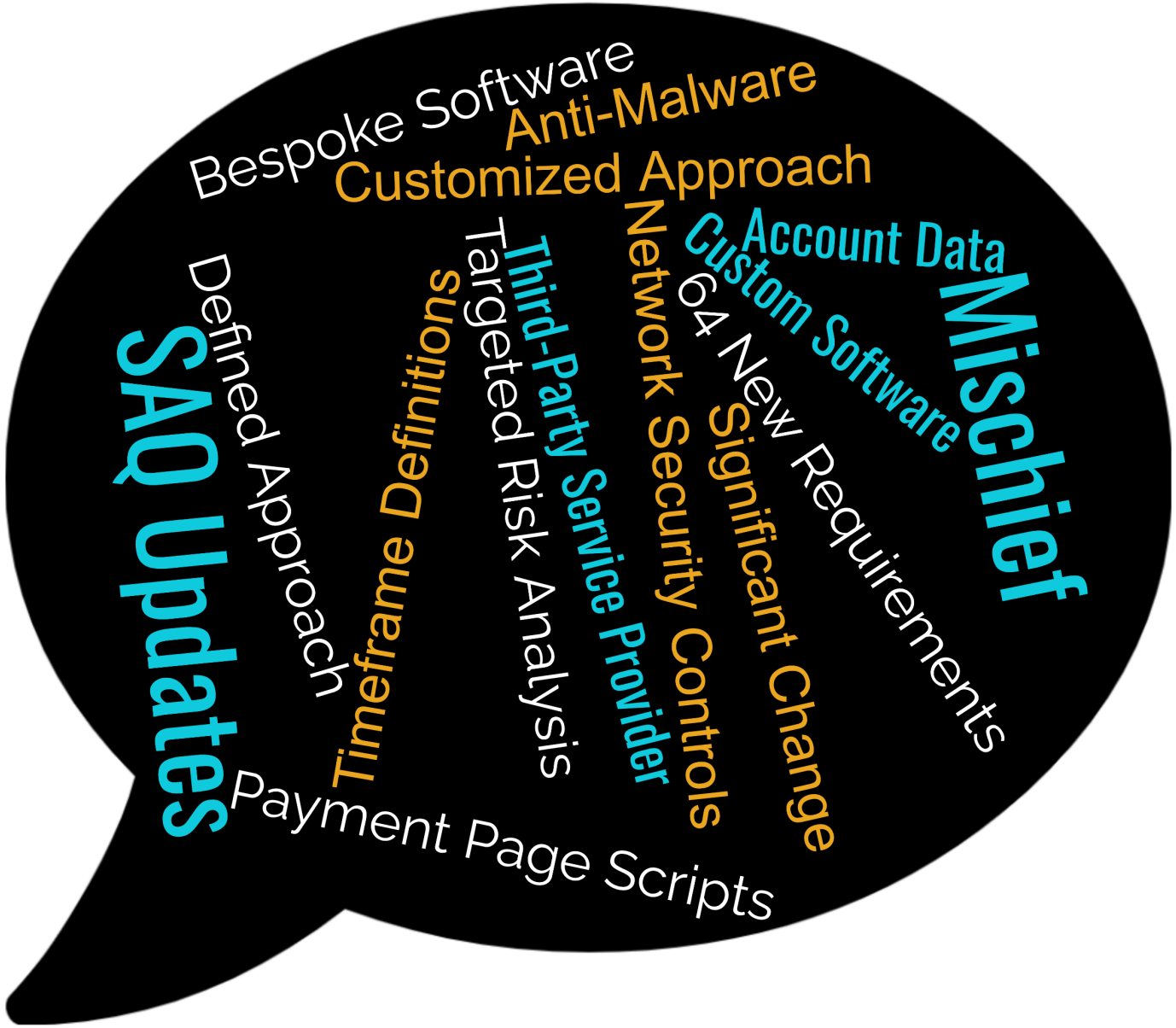


PCI DSS v4.0 Schedule



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

What's New?


Bespoke Software
Anti-Malware
Customized Approach
Account Data
Custom Software
Mischief
Network Security Controls
Significant Change
64 New Requirements
Third-Party Service Provider
Timeframe Definitions
Targeted Risk Analysis
Defined Approach
SAQ Updates
Payment Page Scripts

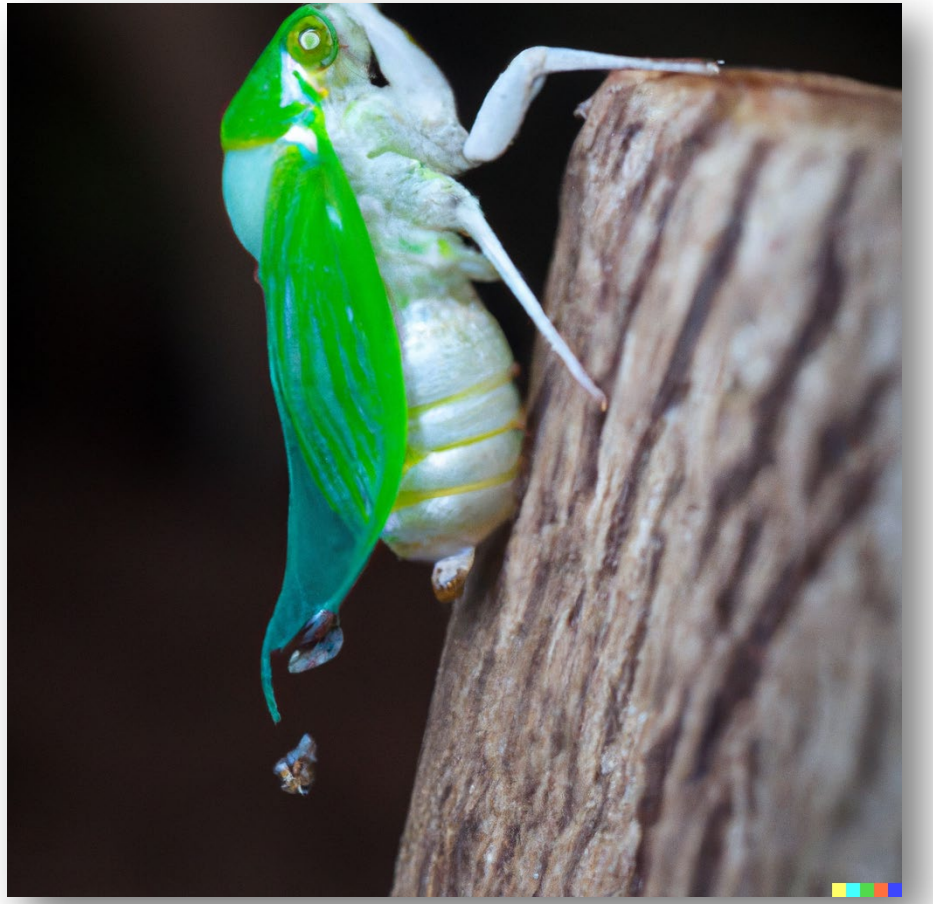
Key Transformations

New Terminology

- Network [illegible] ntrols (NS[illegible])
- Mischief
- Anti-Malware
- Bespoke Softwar[illegible]
- Custom Software
- Payment Page Scripts
- Preproduction

Significant Changes

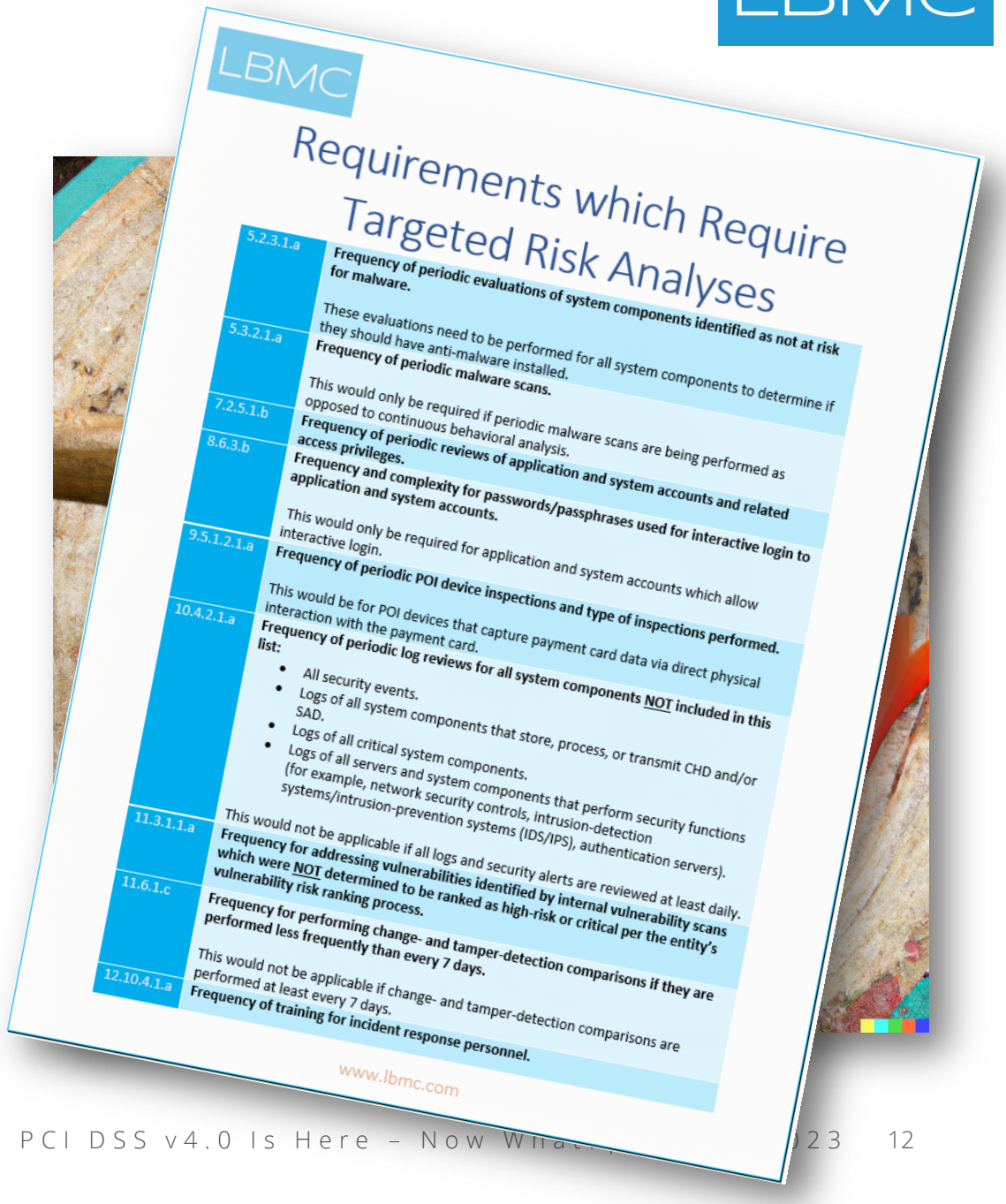
- New hardware or software
- Replacement or major upgrades of hardware and software
- Changes in the flow or storage of account data
- Changes to the scope of the PCI DSS assessment
- Changes to the underlying infrastructure
- Changes to third party service providers



Defined Approach vs Customized Approach

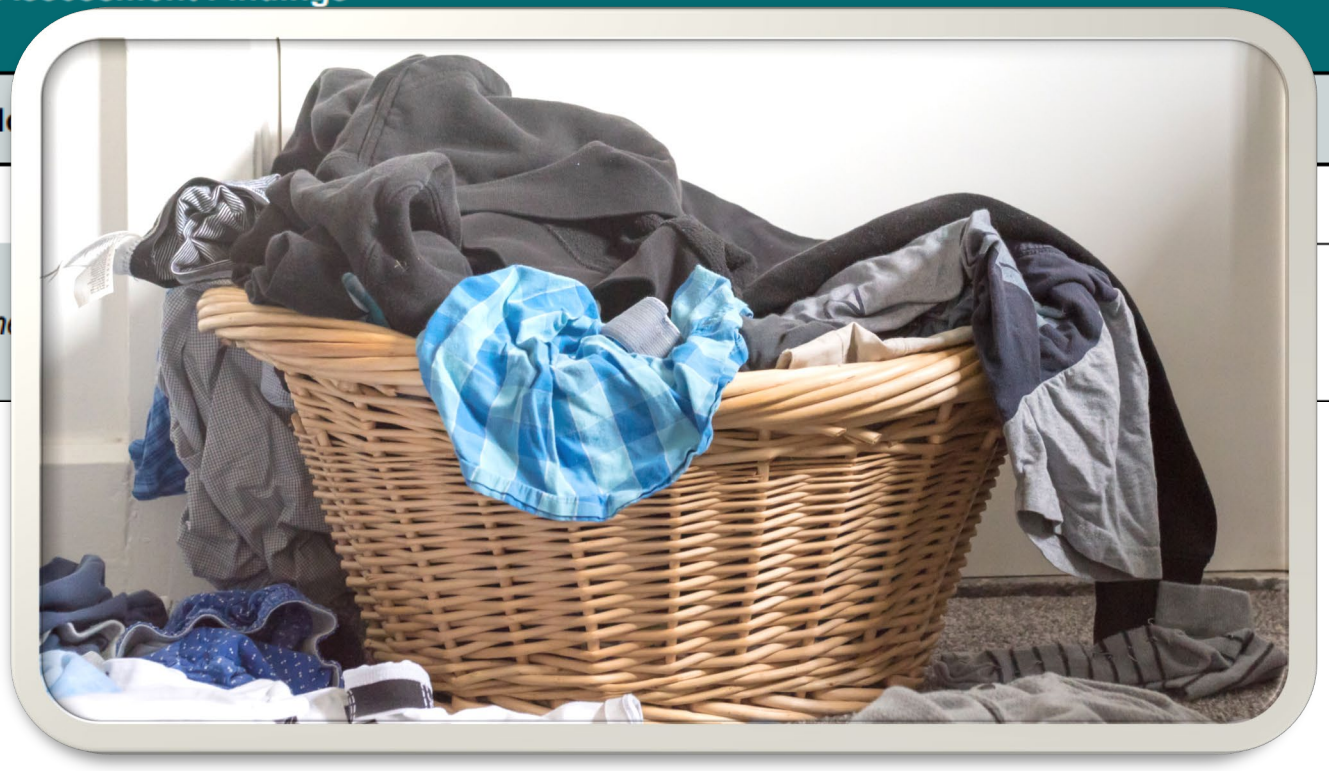
Risk Assessments

- 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



In Place With Remediation

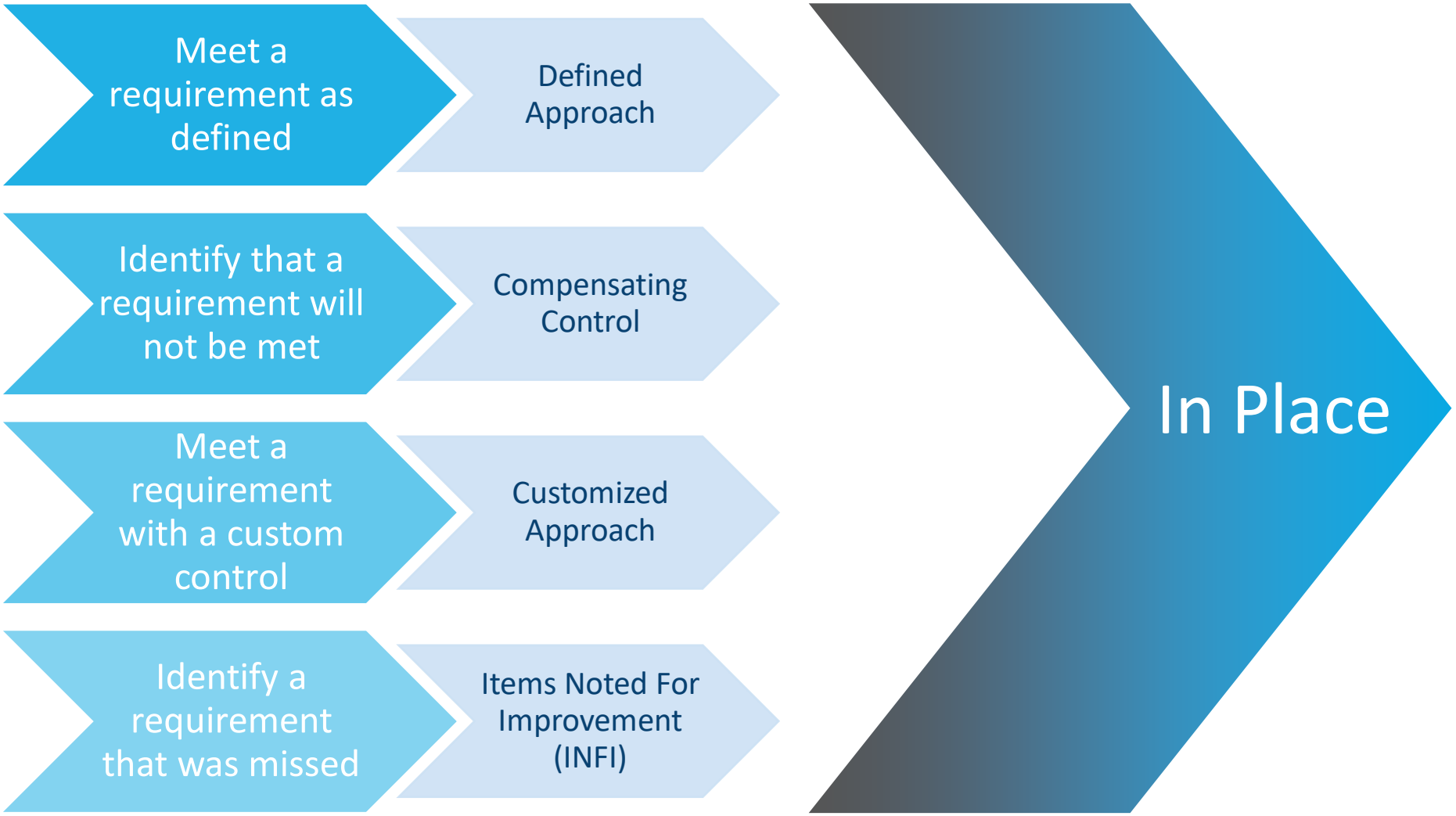
Assessment Findings		
In Place	In Place with Remediation	Not
☐	☐	
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Report... column of the Assessment Findings in the ROC Template Instructions*		



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

Flexible Compliance



Self-Assessment Questionnaire (SAQ) Updates

- All SAQs have been updated
- SAQs include new and updated requirements
- Some SAQs now include additional “old” requirements
- The SAQ-D for Service Providers was significantly updated

Key New Requirements

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)
- Prevention of remote copy of primary account number (PAN)
- Hashes are keyed cryptographic hashes of the entire PAN
- Disk-level encryption is only acceptable for removeable media

Anti-Malware

- Perform scans

  OR

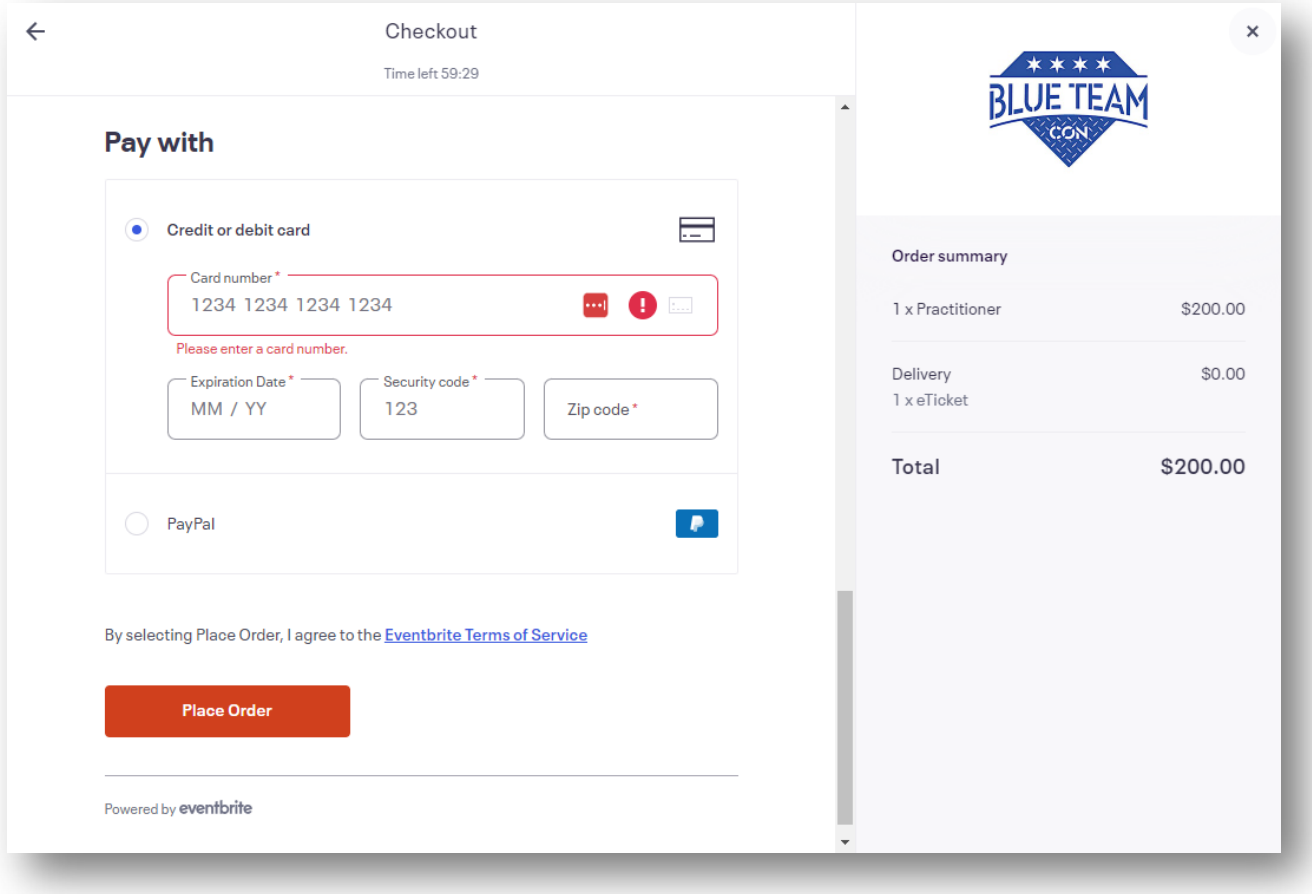
- Perform continuous behavioral analysis of systems or processes
- Removable electronic media (e.g., USB sticks)

Phishing Protection

- Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks
- Security awareness training updates
  - Phishing and related attacks
  - Social engineering

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
- An automated technical solution, such as a web application firewall (WAF) is deployed

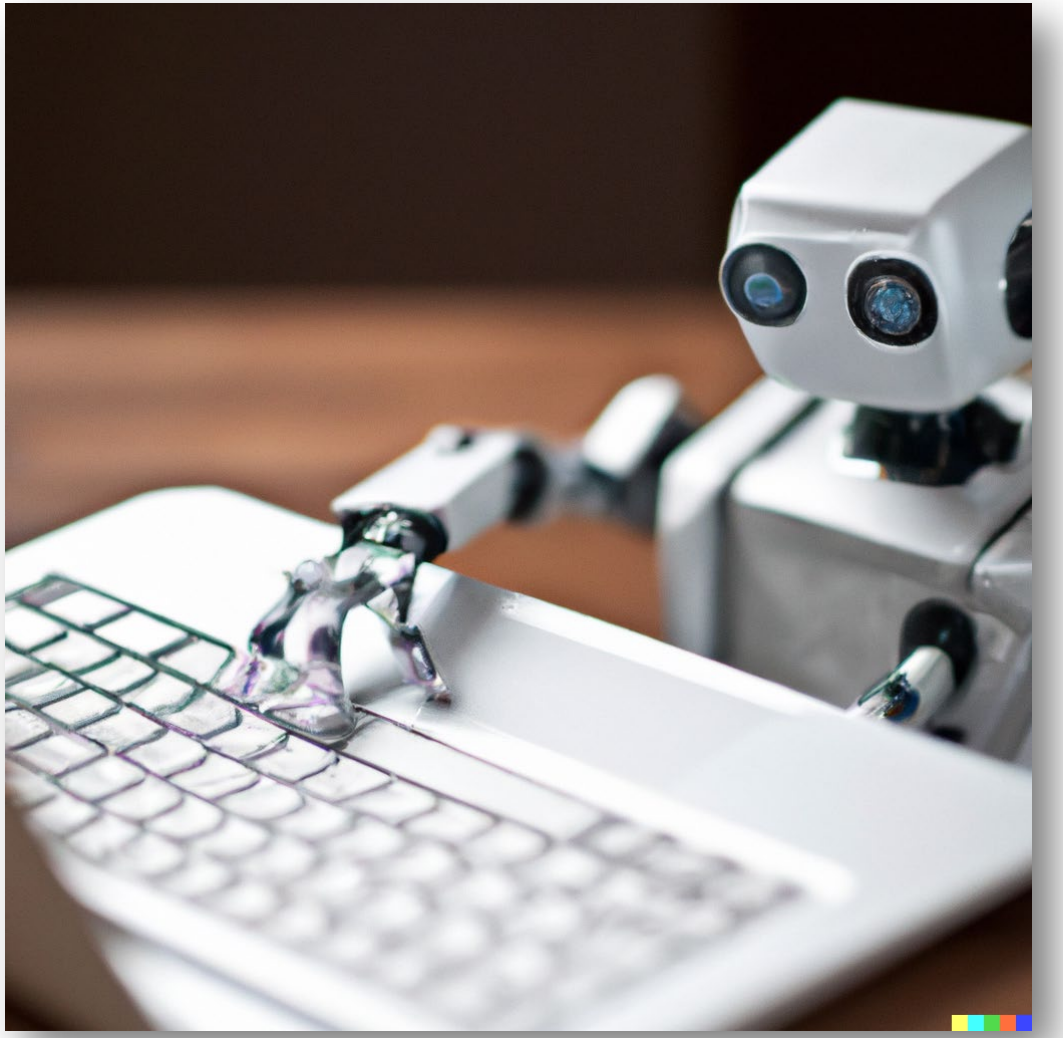


User Account Controls

- 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 for such accounts are not hard coded
- Passwords are changed periodically or upon suspicion/confirmation of compromise
- Passwords have sufficient complexity for how frequently they are changed



Incident Response

- Procedures are in place to be initiated upon the detection of stored primary account number (PAN) anywhere it is not expected

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

Authenticated Internal Vulnerability Scans

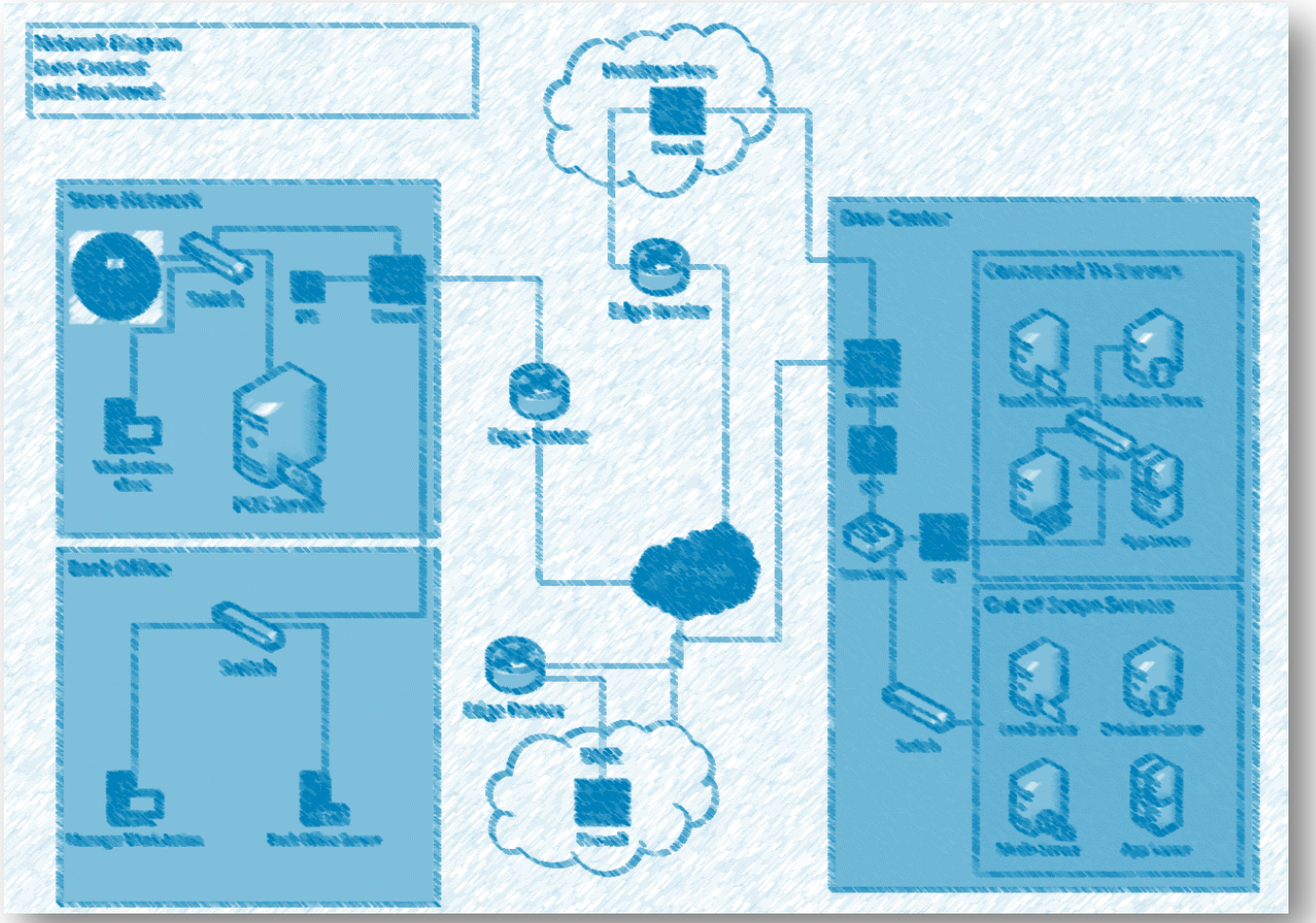
- Internal vulnerability scans are performed via authenticated scanning.

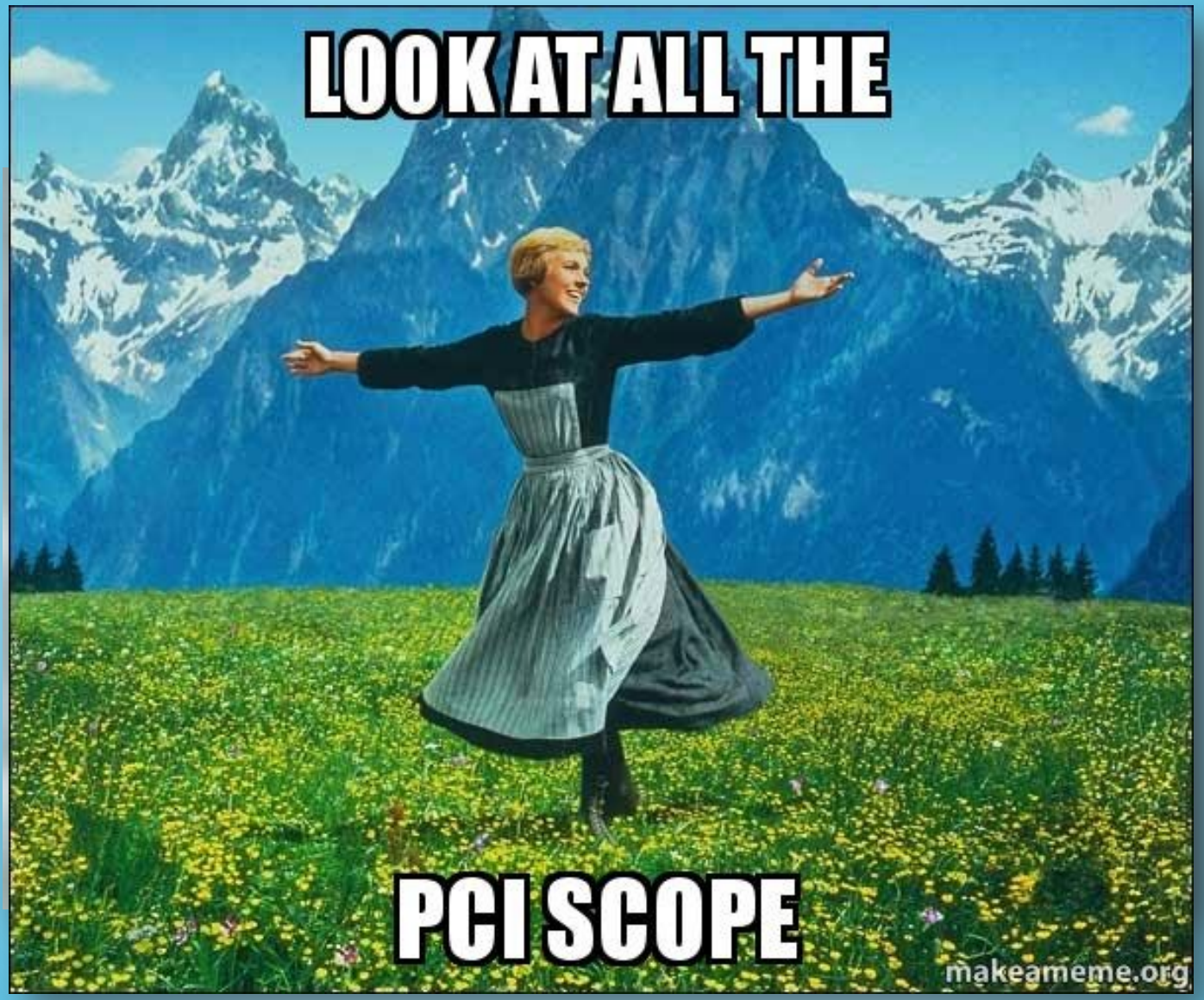
Driving back home after printing out the vulnerability scan report

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^{th} day of the month.
Every three months ("quarterly")	At least once every 90 to 92 days, or on the n^{th} day of each third month.
Every six months	At least once every 180 to 184 days, or on the n^{th} 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.

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




LOOK AT ALL THE
PCI SCOPE
makeameme.org

ANY QUESTIONS?

Kyle Hinterberg, QSA, CISSP, CISA, AWS SCS
Manager, LBMC
kyle.hinterberg@lbmc.com
linkedin.com/in/kylehinterberg

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

CYBERSECURITY SENSE

www.LBMC.com