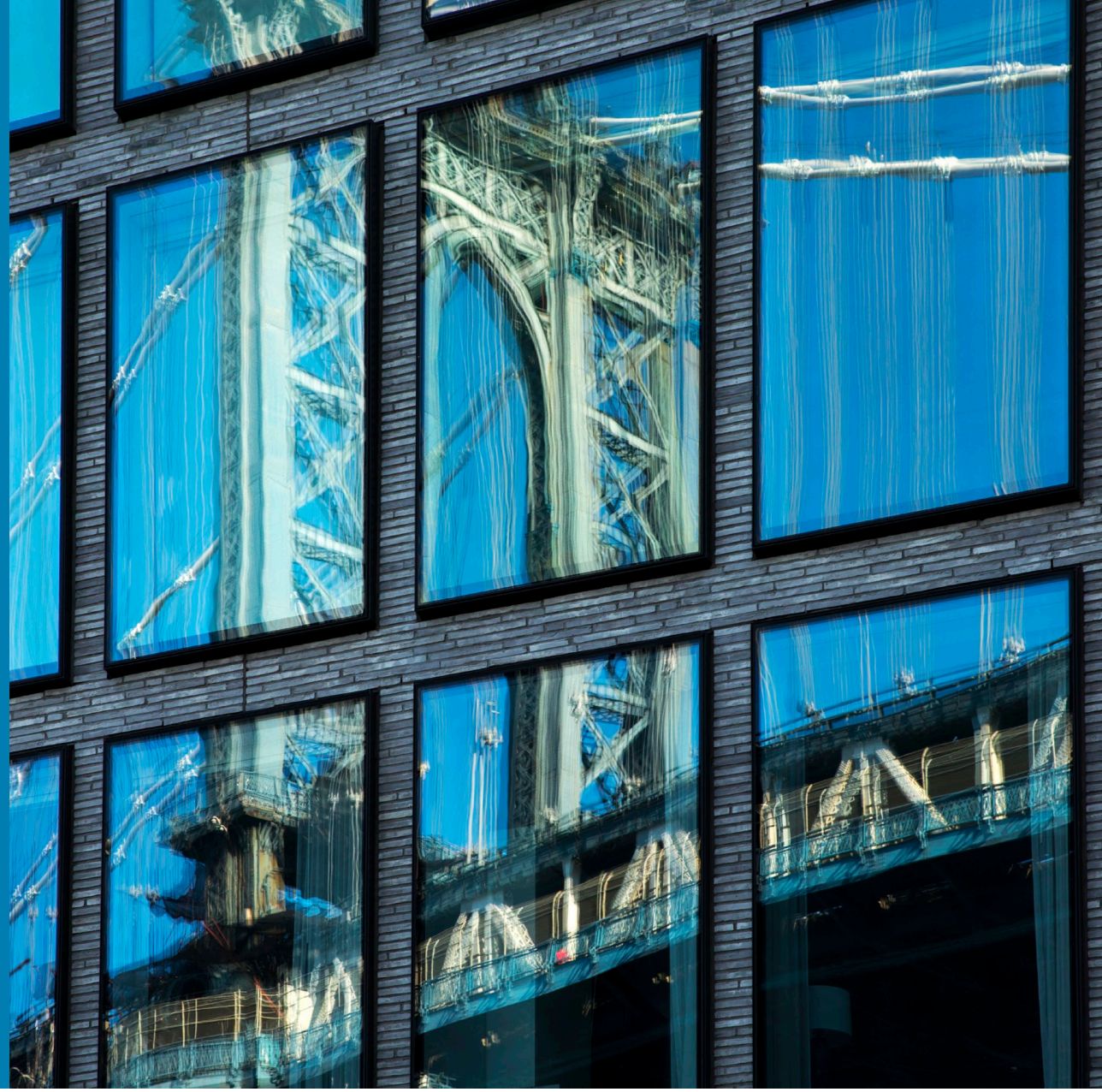
New PCI DSS Requirements: Cardholder Data Handling, Encryption, and Multifactor Authentication

January 24, 2023

Jacob Ansari



mazars

Introductions

Jacob Ansari

Director – Sensitive Data Cybersecurity Compliance

National PCI Practice Lead

Jacob has been performing security assessments and providing security and privacy consulting services for more than twenty years to a variety of industries, including banking and finance, retail, hospitality, technology, and education. Jacob has been leading and performing assessments for PCI DSS compliance for a variety of organizations since the standard's inception, and has a deep, technical level of expertise on the various PCI standards, including the Data Security Standard, PCI PIN, Software Security Framework, and Point-to-Point Encryption

Jacob has extensive experience in penetration testing, application security, forensics and incident response, and risk and governance. He has worked as a CISO, provided risk and strategy guidance to clients and partners, and helped evaluate privacy requirements and integrate privacy, security, and technology functions.

Agenda

01 Overview of new requirements

02 New requirements – cardholder data, encryption, MFA

03 Strategies and solutions

04 Questions and answers

Overview of New Requirements

- Most new requirements (about 55) do not come into effect right away
  - Sunrise after March 31, 2025
  - Considered best practices until then
  - ROC should say something like “This is a best practice and not yet implemented”
- A few requirements come into effect right away with DSS 4.0
  - Covered these in the last webinar
    - We’ll post the link to the slides and video

Overview of New Requirements

- Text and images from the standard comes from PCI DSS standard available at www.pcisecuritystandards.org

Handling Cardholder Data

- Sensitive Authentication Data (SAD)
  - Magnetic stripe or EMV-equivalent data elements
  - Card security codes or values
  - PIN or PIN block data
- Mirrors the requirements for primary account numbers (PANs)
  - Determine your retention requirements
  - Minimum necessary
  - Justification for doing so

Requirements and Testing Procedures	
3.2 Storage of account data is kept to a minimum.	
Defined Approach Requirements	**Defined Approach Testing Procedures**
3.2.1 Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following: • Coverage for all locations of stored account data. • Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details.* • Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements. • Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification.	**3.2.1.a** Examine the data retention and disposal policies, procedures, and processes and interview personnel to verify processes are defined to include all elements specified in this requirement. **3.2.1.b** Examine files and system records on system components where account data is stored to verify that the data storage amount and retention time does not exceed the requirements defined in the data retention policy. **3.2.1.c** Observe the mechanisms used to render account data unrecoverable to verify data cannot be recovered.

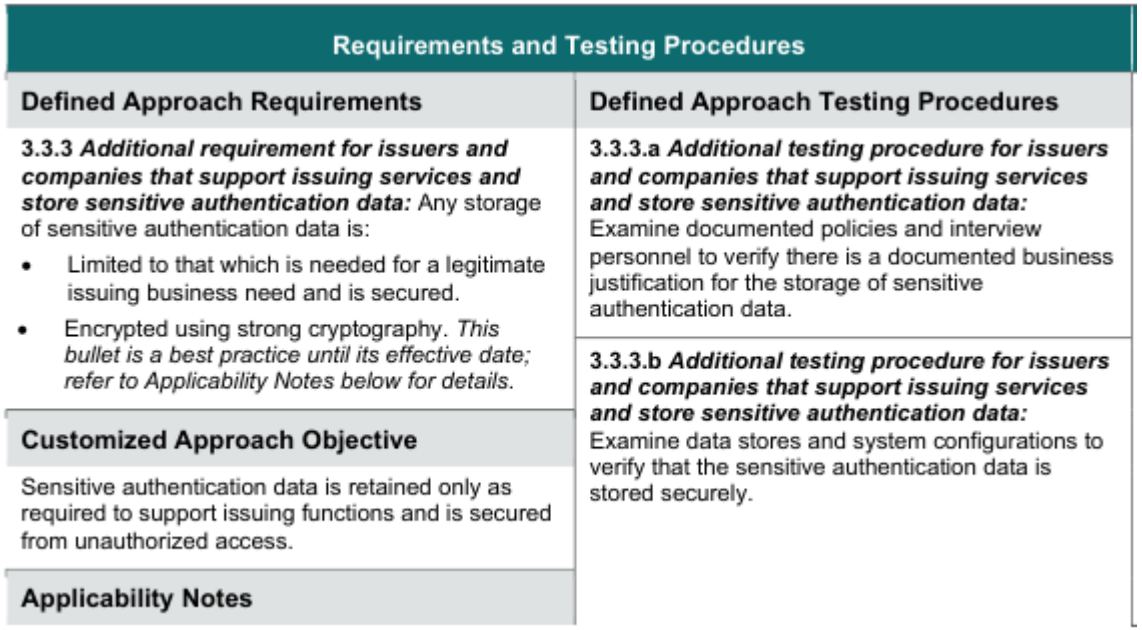
Handling Cardholder Data

- Encryption for SAD:
  - Store-and-forward situations
    - Offline capture
    - Outage scenarios
- Applies the same requirements for PAN to SAD:
  - Really, you should have been doing this already
  - Note the “even if no PAN is present” part
  - Does not supersede requirements in PCI PIN standard

Requirements and Testing Procedures	
Defined Approach Requirements	**Defined Approach Testing Procedures**
3.3.2 SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography.	**3.3.2** Examine data stores, system configurations, and/or vendor documentation to verify that all SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography.
Customized Approach Objective	
This requirement is not eligible for the customized approach.	
Applicability Notes	
Whether SAD is permitted to be stored prior to authorization is determined by the organizations that manage compliance programs (for example, payment brands and acquirers). Contact the organizations of interest for any additional criteria. This requirement applies to all storage of SAD, even if no PAN is present in the environment. Refer to Requirement 3.2.1 for an additional requirement that applies if SAD is stored prior to completion of authorization. This requirement does not apply to issuers and companies that support issuing services where there is a legitimate issuing business justification to store SAD). Refer to Requirement 3.3.3 for requirements specifically for issuers. This requirement does not replace how PIN blocks are required to be managed, nor does it mean that a properly encrypted PIN block needs to be encrypted again. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	

Handling Cardholder Data

- New requirements for issuers and those who support issuing services:
  - Can retain SAD *after* authorization
  - Same principles as existing PCI DSS requirements
  - Again, probably should already be in place



Requirements and Testing Procedures	
Defined Approach Requirements	**Defined Approach Testing Procedures**
3.3.3 ***Additional requirement for issuers and companies that support issuing services and store sensitive authentication data:*** Any storage of sensitive authentication data is: • Limited to that which is needed for a legitimate issuing business need and is secured. • Encrypted using strong cryptography. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details.*	**3.3.3.a** ***Additional testing procedure for issuers and companies that support issuing services and store sensitive authentication data:*** Examine documented policies and interview personnel to verify there is a documented business justification for the storage of sensitive authentication data.
Customized Approach Objective	**3.3.3.b** ***Additional testing procedure for issuers and companies that support issuing services and store sensitive authentication data:*** Examine data stores and system configurations to verify that the sensitive authentication data is stored securely.
Sensitive authentication data is retained only as required to support issuing functions and is secured from unauthorized access.	
Applicability Notes	

A brief detour on masking

- Masking requirements in DSS 3.2.1 – limit to display first six and last four digits
- Masking in DSS 4.0 (Req 3.4.1) – Maximum digits displayed are the BIN and the last four digits
  - Bank Identification Number – not necessarily six digits any longer
  - Some business cases need to display the full BIN
  - Does not supersede existing requirements for stricter masking:
    - Payment brand requirements
    - Laws or other regulations (e.g., customer receipts)

Remote access to cardholder data through the ages

- Do you remember Requirement 12.3.10?
  - **Policy** requirement to prohibit copy/paste using remote access
    - Requirement 12.3 began life in the early 2000s as controls around modems
  - Didn't have any enforcement mechanisms at the actual systems themselves

PCI Security Standards Council

PCI DSS Requirements	Testing Procedures	
12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.	**12.3.10.a** Verify that the usage policies prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies. **12.3.10.b** For personnel with proper authorization, verify that usage policies require the protection of cardholder data in accordance with PCI DSS Requirements.	To re da m ac ex ca m PC

Note: this is from PCI DSS v3.2.1

Remote access to cardholder data through the ages

- This idea migrated to Requirement 3.4.2:
  - **Technical controls** required to prohibit copy/paste **or relocation** using remote access
  - Prohibited except for explicit authorization and defined business need
  - Applicable if it's *possible*, not just if it's *intended*

Requirements and Testing Procedures	
Defined Approach Requirements	**Defined Approach Testing Procedures**
3.4.2 When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need.	**3.4.2.a** Examine documented policies and procedures and documented evidence for technical controls that prevent copy and/or relocation of PAN when using remote-access technologies onto local hard drives or removable electronic media to verify the following: • Technical controls prevent all personnel not specifically authorized from copying and/or relocating PAN. • A list of personnel with permission to copy and/or relocate PAN is maintained, together with the documented, explicit authorization and legitimate, defined business need.
Customized Approach Objective	
PAN cannot be copied or relocated by unauthorized personnel using remote-access technologies.	
Applicability Notes	**3.4.2.b** Examine configurations for remote-access technologies to verify that technical controls to prevent copy and/or relocation of PAN for all personnel, unless explicitly authorized.
Storing or relocating PAN onto local hard drives, removable electronic media, and other storage devices brings these devices into scope for PCI DSS. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	**3.4.2.c** Observe processes and interview personnel to verify that only personnel with documented, explicit authorization and a legitimate, defined business need have permission to copy and/or relocate PAN when using remote-access technologies.

How do we solve for this?

- Controls can be applied at the remote access layer or at the target system layer
  - Remote access system design needs to account for this level of granularity
  - File-level permissions may be a part of the solution
- Must be **preventative** and not detective controls
  - Existing integrity monitoring or HIDS are not sufficient by themselves
  - Customized approach might be useful here: still needs to be **preventative**

Keyed cryptographic hashes

- Hashes used to render PAN unreadable must use keyed hash function (e.g., HMAC, CMAC)
  - Cannot rely on just a hash function any longer
- Will affect lookup table functionality (e.g., known bad card numbers)
- Possible performance impact for token vaults or similar usage

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** The removal of cleartext stored PAN is a defense in depth control designed to protect the data if an unauthorized individual gains access to stored data by taking advantage of a vulnerability or misconfiguration of an entity's primary access control. Secondary independent control systems (for example governing access to, and use of, cryptography and decryption keys) prevent the failure of a primary access control system leading to a breach of confidentiality of stored PAN. **Good Practice** A hashing function that incorporates a randomly generated secret key provides brute force attack resistance and secret authentication integrity. **Further Information** Appropriate keyed cryptographic hashing algorithms include but are not limited to: HMAC, CMAC, and GMAC, with an effective cryptographic strength of at least 128-bits (*NIST SP 800-131Ar2*). Refer to the following for more information about HMAC, CMAC, and GMAC, respectively: *NIST SP 800-107r1, NIST SP 800-38B, and NIST SP 800-38D).* See *NIST SP 800-107 (Revision 1): Recommendation for Applications Using Approved Hash Algorithms* §5.3.
3.5.1.1 Hashes used to render PAN unreadable (per the first bullet of Requirement 3.5.1) are keyed cryptographic hashes of the entire PAN, with associated key-management processes and procedures in accordance with Requirements 3.6 and 3.7.	**3.5.1.1.a** Examine documentation about the hashing method used to render PAN unreadable, including the vendor, type of system/process, and the encryption algorithms (as applicable) to verify that the hashing method results in keyed cryptographic hashes of the entire PAN, with associated key management processes and procedures.	
Applicability Notes	**3.5.1.1.b** Examine documentation about the key management procedures and processes associated with the keyed cryptographic hashes to verify keys are managed in accordance with Requirements 3.6 and 3.7.	
This requirement applies to PANs stored in primary storage (databases, or flat files such as text files spreadsheets) as well as non-primary storage (backup, audit logs, exception, or troubleshooting logs) must all be protected. This requirement does not preclude the use of temporary files containing cleartext PAN while encrypting and decrypting PAN. *This requirement is considered a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	**3.5.1.1.c** Examine data repositories to verify the PAN is rendered unreadable.	
	3.5.1.1.d Examine audit logs, including payment application logs, to verify the PAN is rendered unreadable.	

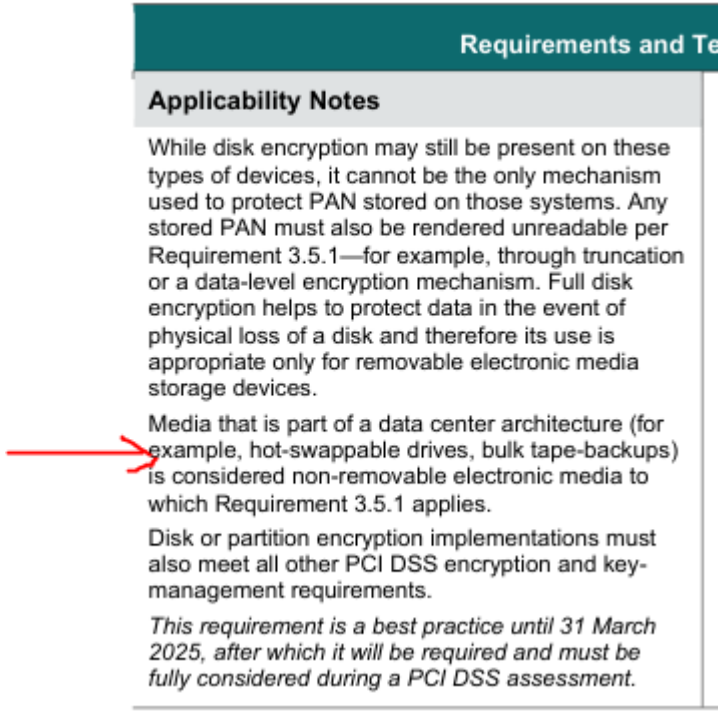
Disk encryption – closing the loophole

- Disk encryption is now only suitable for:
  - Removable media
  - In conjunction with another means of rendering PAN unreadable
- Disk encryption for always-on systems has been largely ineffective for years
  - When disks are mounted, the data are decrypted
  - Minimal protections in these circumstances

Requirements and Testing Procedures	
Defined Approach Requirements	**Defined Approach Testing Procedures**
3.5.1.2 If disk-level or partition-level encryption (rather than file-, column-, or field-level database encryption) is used to render PAN unreadable, it is implemented only as follows: • On removable electronic media **OR** • If used for non-removable electronic media, PAN is also rendered unreadable via another mechanism that meets Requirement 3.5.1.	**3.5.1.2.a** Examine encryption processes to verify that, if disk-level or partition-level encryption is used to render PAN unreadable, it is implemented only as follows: • On removable electronic media, **OR** • If used for non-removable electronic media, examine encryption processes used to verify that PAN is also rendered unreadable via another method that meets Requirement 3.5.1.
Customized Approach Objective	**3.5.1.2.b** Examine configurations and/or vendor documentation and observe encryption processes to verify the system is configured according to vendor documentation the result is that the disk or the partition is rendered unreadable.
This requirement is not eligible for the customized approach. *(continued on next page)*	

Disk encryption – closing the loophole

- Bulk backup media and hot-swap drives are non-removable media
  - This requirement applies here
- Many disk encryption use cases will need additional controls
  - Encrypting the data element itself
  - Even valid use cases require PCI DSS key management requirements



Requirements and Te

Applicability Notes

While disk encryption may still be present on these types of devices, it cannot be the only mechanism used to protect PAN stored on those systems. Any stored PAN must also be rendered unreadable per Requirement 3.5.1—for example, through truncation or a data-level encryption mechanism. Full disk encryption helps to protect data in the event of physical loss of a disk and therefore its use is appropriate only for removable electronic media storage devices.

Media that is part of a data center architecture (for example, hot-swappable drives, bulk tape-backups) is considered non-removable electronic media to which Requirement 3.5.1 applies.

Disk or partition encryption implementations must also meet all other PCI DSS encryption and key-management requirements.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

Disk encryption – closing the loophole

- Existing disk encryption controls still remain:
  - Logical access is managed separately from the operating system
  - Decryption keys not associated with the operating system
  - Store secrets securely

Requirements and Testing Procedures	
Defined Approach Requirements	**Defined Approach Testing Procedures**
3.5.1.3 If disk-level or partition-level encryption is used (rather than file-, column-, or field--level database encryption) to render PAN unreadable, it is managed as follows: • Logical access is managed separately and independently of native operating system authentication and access control mechanisms. • Decryption keys are not associated with user accounts. • Authentication factors (passwords, passphrases, or cryptographic keys) that allow access to unencrypted data are stored securely.	**3.5.1.3.a** If disk-level or partition-level encryption is used to render PAN unreadable, examine the system configuration and observe the authentication process to verify that logical access is implemented in accordance with all elements specified in this requirement. **3.5.1.3.b** Examine files containing authentication factors (passwords, passphrases, or cryptographic keys) and interview personnel to verify that authentication factors that allow access to unencrypted data are stored securely and are independent from the native operating system's authentication and access control methods.
Customized Approach Objective	
Disk encryption implementations are configured to require independent authentication and logical access controls for decryption.	
Applicability Notes	
Disk or partition encryption implementations must also meet all other PCI DSS encryption and key-management requirements.	

Minor key management update

- For service providers:
  - Cryptographic architecture requirement (3.6.1.1) - cannot use of the same keys in both production and test

Data in transmission – keys and certificates

- Certificates must be valid and not expired or revoked
  - Issued by a trusted source like a CA
    - Can be an internal CA
    - Issued-by must not equal issued-to
- Certificate or key pinning may be used to validate
- Maintain inventory of trusted keys and certificates
  - Algorithms, protocols, key strength, custodians, expiry dates

Requirements and Testing Procedures	
4.2 PAN is protected with strong cryptography during transmission.	
Defined Approach Requirements	**Defined Approach Testing Procedures**
4.2.1 Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks: • Only trusted keys and certificates are accepted. • Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked. *This bullet is a best practice until its effective date; refer to applicability notes below for details.* • The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations. • The encryption strength is appropriate for the encryption methodology in use.	**4.2.1.a** Examine documented policies and procedures and interview personnel to verify processes are defined to include all elements specified in this requirement. **4.2.1.b** Examine system configurations to verify that strong cryptography and security protocols are implemented in accordance with all elements specified in this requirement. **4.2.1.c** Examine cardholder data transmissions to verify that all PAN is encrypted with strong cryptography when it is transmitted over open, public networks. **4.2.1.d** Examine system configurations to verify that keys and/or certificates that cannot be verified as trusted are rejected.
Customized Approach Objective	
Cleartext PAN cannot be read or intercepted from any transmissions over open, public networks.	

Multifactor authentication (MFA) – the main event

- Changes to MFA usage occur in two places:
  - 8.4.2 – All access into the CDE, except:
    - Application or system accounts – automated functions
    - User accounts on POS terminals
  - 8.4.3 – Remote access from outside that could access or impact the CDE:
    - All personnel
    - Third parties and vendors

Requirements and Testing Procedures	
Defined Approach Requirements	**Defined Approach Testing Procedures**
8.4.2 MFA is implemented for all access into the CDE.	**8.4.2.a** Examine network and/or system configurations to verify MFA is implemented for all access into the CDE.
	8.4.2.b Observe personnel logging in to the CDE and examine evidence to verify that MFA is required.
Customized Approach Objective	
Access into the CDE cannot be obtained by the use of a single authentication factor.	
Applicability Notes	
This requirement does not apply to: • Application or system accounts performing automated functions. • User accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals). MFA is required for both types of access specified in Requirements 8.4.2 and 8.4.3. Therefore, applying MFA to one type of access does not replace the need to apply another instance of MFA to the other type of access. If an individual first connects to the entity's network via remote access, and then later initiates a connection into the CDE from within the network, per this requirement the individual would authenticate using MFA twice, once when connecting via remote access to the entity's network and once when connecting via non-console administrative access from the entity's network into the CDE. *(continued on next page)*	

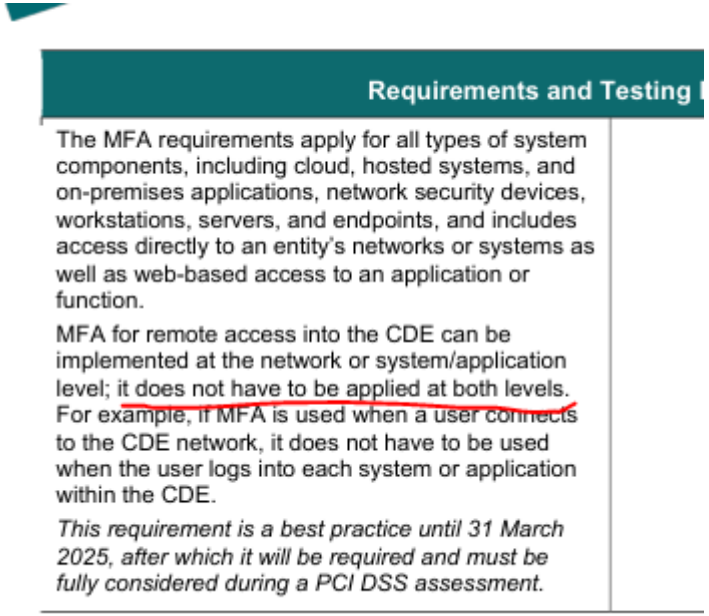
Multifactor authentication (MFA) – the main event

- Changes to MFA usage occur in two places:
  - 8.4.2 – All access into the CDE, except:
    - Application or system accounts – automated functions
    - User accounts on POS terminals
  - 8.4.3 – Remote access from outside that could access or impact the CDE:
    - All personnel
    - Third parties and vendors

Defined Approach Requirements	Defined Approach Testing Procedures
8.4.3 MFA is implemented for all remote network access originating from outside the entity's network that could access or impact the CDE as follows: • All remote access by all personnel, both users and administrators, originating from outside the entity's network. • All remote access by third parties and vendors.	**8.4.3.a** Examine network and/or system configurations for remote access servers and systems to verify MFA is required in accordance with all elements specified in this requirement.
	8.4.3.b Observe personnel (for example, users a administrators) connecting remotely to the netwo and verify that multi-factor authentication is required.
Customized Approach Objective	
Remote access to the entity's network cannot be obtained by using a single authentication factor.	
Applicability Notes	
The requirement for MFA for remote access originating from outside the entity's network applies to all user accounts that can access the network remotely, where that remote access leads to or could lead to access into the CDE. If remote access is to a part of the entity's network that is properly segmented from the CDE, such that remote users cannot access or impact the CDE, MFA for remote access to that part of the network is not required. However, MFA is required for any remote access to networks with access to the CDE and is recommended for all remote access to the entity's networks. The MFA requirements apply for all types of system components, including cloud, hosted systems, and on-premises applications, network security devices, workstations, servers, and endpoints, and includes access directly to an entity's networks or systems as well as web-based access to an application or function.	

A few considerations

- For 8.4.2 – MFA can occur at the network layer and not at each individual system
  - May be necessary for certain device types
- Beware of two-step authentication:
  - One factor grants access to the other
    - Common implementations of SSH keys



Requirements and Testing
The MFA requirements apply for all types of system components, including cloud, hosted systems, and on-premises applications, network security devices, workstations, servers, and endpoints, and includes access directly to an entity's networks or systems as well as web-based access to an application or function.
MFA for remote access into the CDE can be implemented at the network or system/application level; it does not have to be applied at both levels. For example, if MFA is used when a user connects to the CDE network, it does not have to be used when the user logs into each system or application within the CDE.
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

A few considerations

- “I’m using a service provider for authentication services”
  - These entities *affect the security* of the cardholder data environment
  - Relevant to PCI DSS scope
    - Treat like a third-party service provider per DSS 12.8
- You should also consider credential repositories like password vaults

Strategies for Implementation

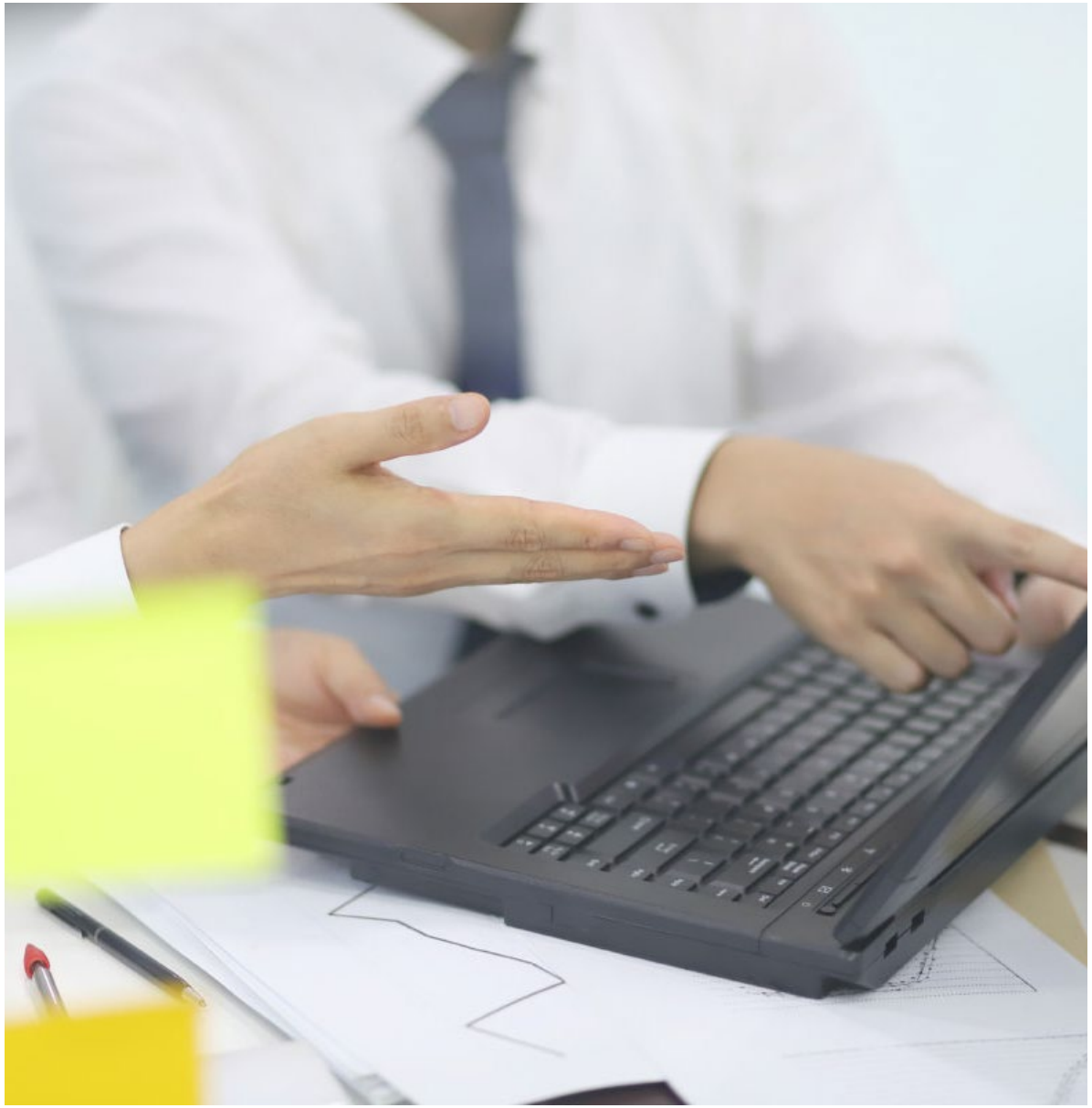
- Start your design process now
  - Understand the use cases
    - MFA: Changing behavior and process > changing tech
  - Involve your assessor in the design:
    - You want their approval before major projects
      - Mindful of independence requirements
      - Maybe you need another assessor for implementation help
  - Consider where the customized approach can help
    - Probably best to use this sparingly
- Use the time wisely

Now for the good part

- **Please ask your questions**
  - Sanitize the identifying details
  - Understand the limits of what we can accomplish here

Future Events – Europrivacy Webinar

- **This week Thursday**
  - Hosted by Mazars Ireland
    - Protecting payment data is fulfilling GDPR obligations
    - Understand how this can help with your privacy obligations
    - http://maza.rs/6045eFwN7



Future Events – Focusing on New Requirements

- **March 21st at 11am EST**
  - Web application and payment page security (Reqs 6, 11)
  - User account and password management (Reqs 7, 8)
  - Endpoint security and phishing protection (Req 5, 12)

- **May 23rd at 11 am EST**
  - Audit log reviews (Req 10)
  - Vulnerability and security control management (Reqs 10, 11)
  - Governance, procedures, scope (Req 12)

Contact

Jacob Ansari
National PCI Practice Leader
jacob.ansari@mazarsusa.com
+1 (267) 532-4388

About Mazars
Mazars is an internationally integrated partnership, specialising in audit, accountancy, advisory, tax and legal services*. Operating in over 90 countries and territories around the world, we draw on the expertise of more than 44,000 professionals – 28,000+ in Mazars' integrated partnership and 16,000+ via the Mazars North America Alliance – to assist clients of all sizes at every stage in their development.

*Where permitted under applicable country laws

Mazars USA LLP
Mazars USA LLP is an independent member firm of Mazars Group, an international audit, tax and advisory organization with operations in over 90 countries. With roots going back to 1921 in the US, the firm has significant national presence in strategic geographies, providing seamless access to 28,000+ professionals around the world. Our industry specialists deliver tailored services to a wide range of clients across sectors, including individuals, high-growth emerging companies, privately-owned businesses and large enterprises.

www.mazars.us

Follow us:

LinkedIn:
www.linkedin.com/company/mazarsinus

Twitter:
www.twitter.com/mazarsinus

Facebook:
www.facebook.com/mazarsinus

Instagram:
www.instagram.com/mazarsinus

mazars

What happened to compensating controls?

- Compensating controls are still around
- Used for a documented business or technical constraint
  - Again, still not the vehicle for “oops, we forgot to run scans”
- Needs the same characteristics as before:
  - Constraint
  - Risk assessment
  - Meet the intent and rigor of the original control
  - Address additional risk
  - Demonstration of evidence and sustainability

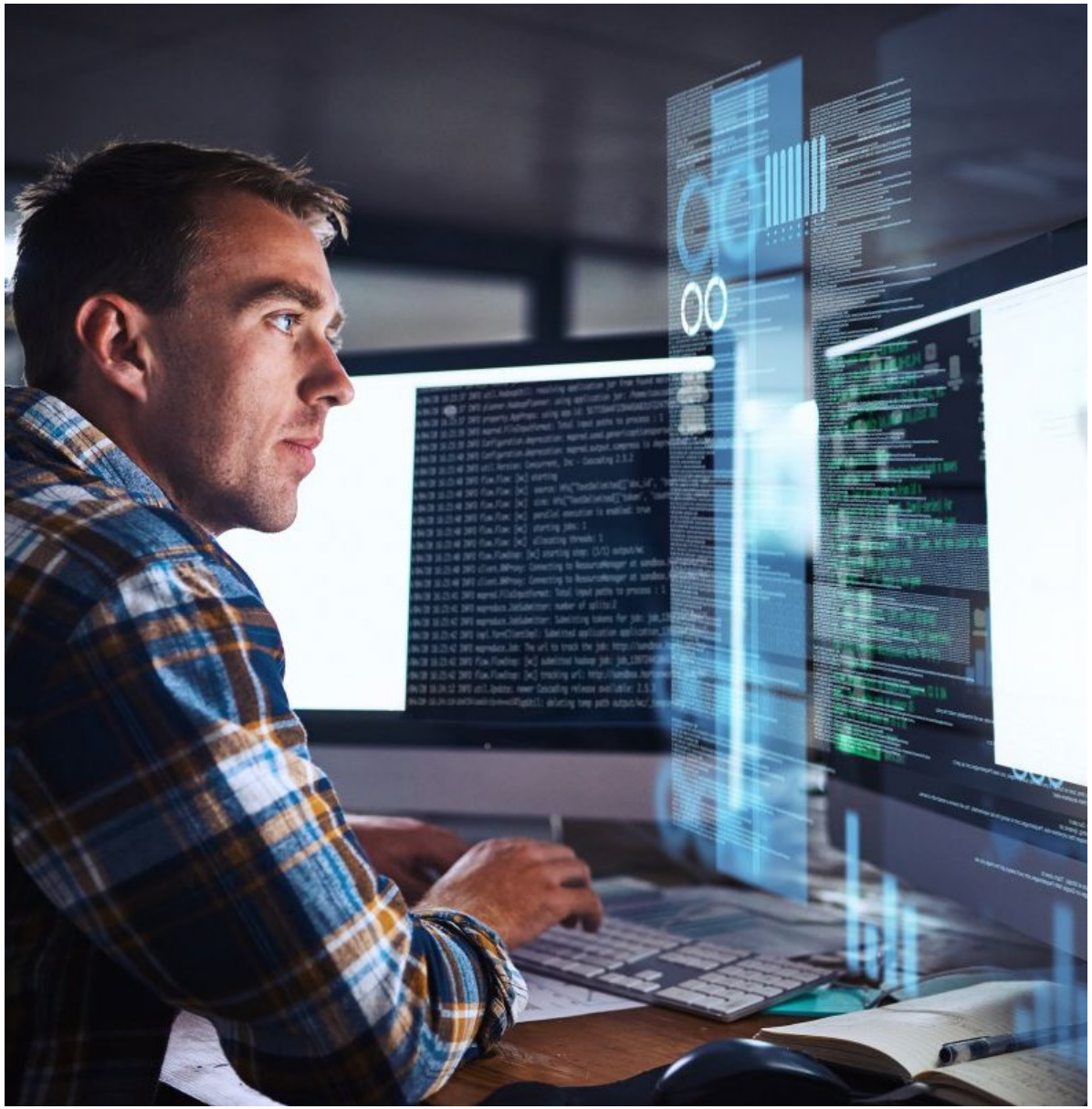
Ok, so new requirements?

- **Roles and responsibilities are documented, assigned, understood**
  - On a per-Requirement basis for the major requirements
  - Effective immediately with DSS 4.0
    - Really, you should have been doing this already

- **If you're using the customized approach:**
  - 12.3.2 – Targeted risk analysis for each requirement
    - Determine how to meet with the customized approach
    - Identify frequency of recurring activities
    - Must perform this TRA once every 12 months

But wait, there’s more

- Several other new requirements
- Considered best practices until March 31, 2025
  - You don’t have to do them until then
  - You need to start preparing for them now
- Details are topics for future webinars
  - Selection of new requirements in subsequent slides

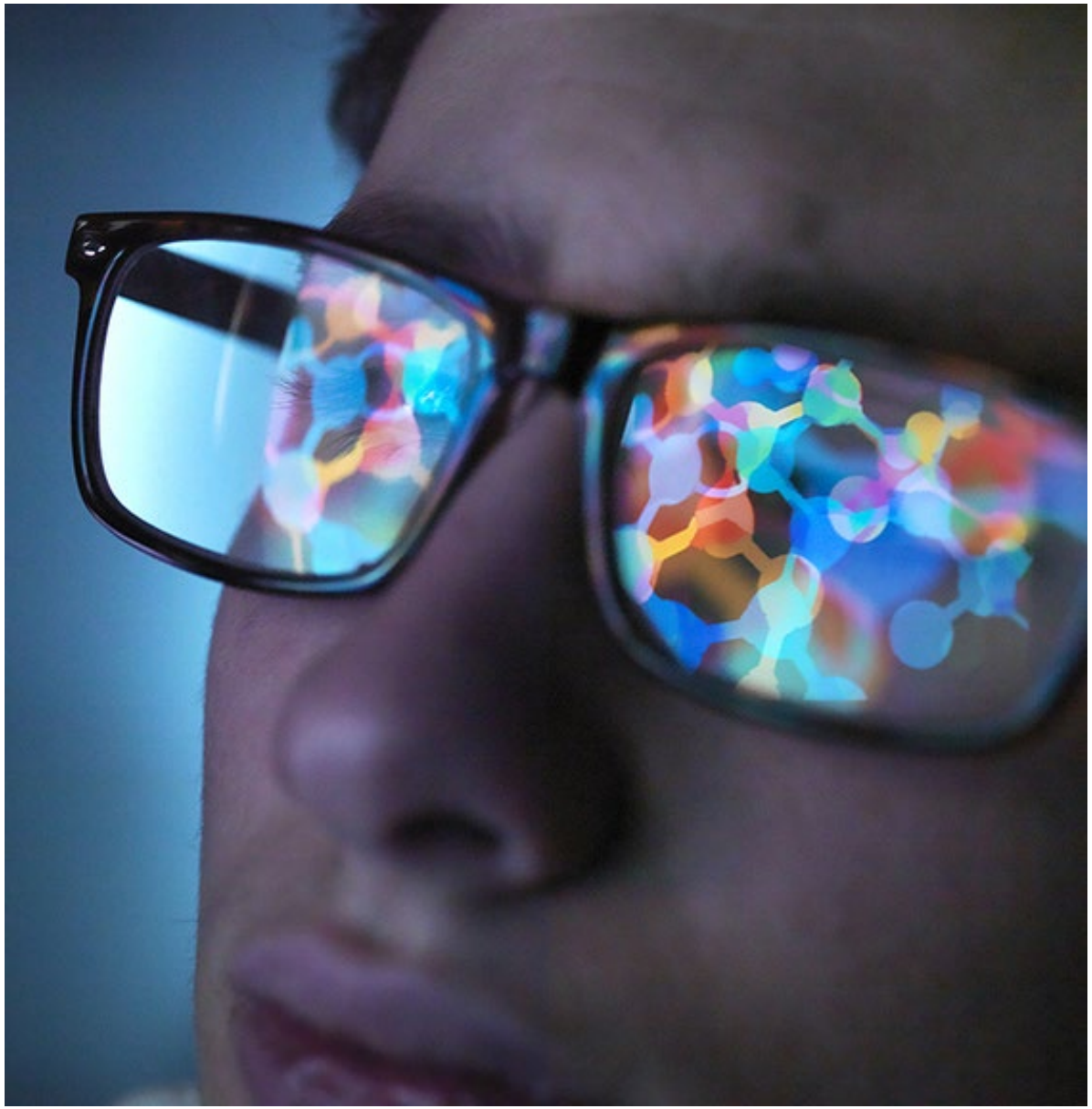


Card Data and Cryptographic Requirements

- **Technical controls to prevent remote access copy/paste of PAN**
  - Except for explicit authorization
  - Might take substantial engineering efforts
- **Hashes used to protect PAN must use keyed cryptographic hash**
  - Affects lookup tables and tokenization functions
  - Will require substantial engineering efforts
- **Disk encryption by itself is only good for removable media**
  - Hot-swap drives or bulk tape backups are considered non-removable

Multifactor Authentication

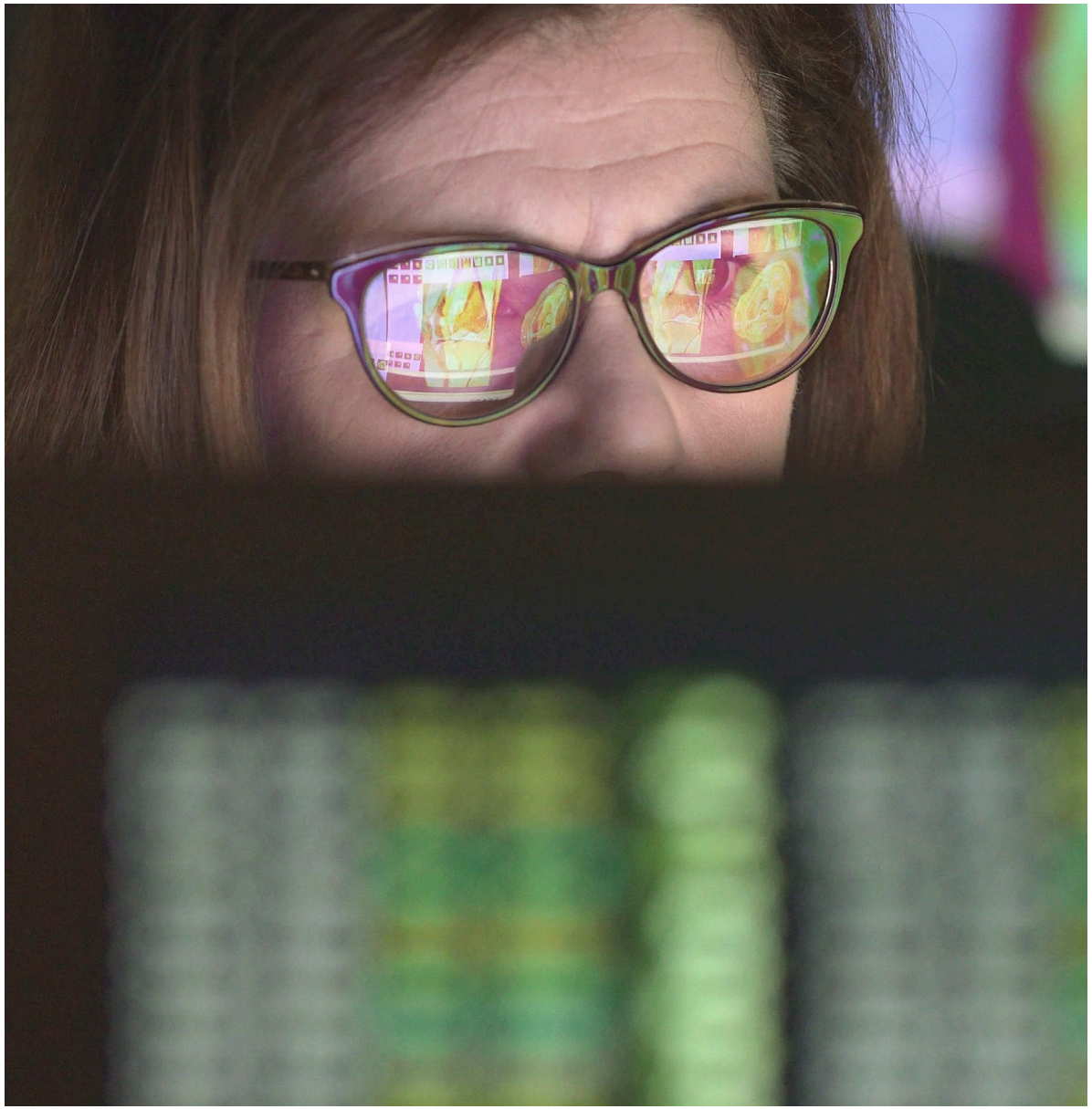
- **Required for all access into CDE**
  - Excepts automated processes and POS devices
- **Required for all remote access from outside entity's network that could access or impact CDE**
  - Possibly draw in third parties that service adjacent networks



Logging and Integrity Management

- **Log analysis must be automated**
  - Cleans up an old loophole that didn't prohibit manual review of logs
    - Has been infeasible for years

- **Change and tamper detection controls for payment pages**
  - Make sure you know where all the Javascript is coming from on payment pages
    - Addresses modern ecommerce skimming attacks



Other considerations

- **Some new compliance states:**
  - Per requirement: In Place With Remediation
    - Intended to identify when remediation activities took place during the assessment
    - This has caused some controversy already
  - Overall: Full or Partial Assessment
    - Partial Assessment = Any requirements marked as Not Tested
    - Can still be compliant with Not Tested, but need to mark Partial Assessment
      - ➢ Useful for entities that only cover some requirements

Timelines and Strategies

- **Current version of PCI DSS (v3.2.1) good until March 31, 2024**
  - Both versions are valid currently
- **Future dated requirements come into effect after March 31, 2025**
  - Requirements are best practices until then

Timelines and Strategies

- **Probably best strategy to stick with 3.2.1 for your next assessment**
  - Start working on gap assessment and readiness for 4.0 now
- **Identify your deficiencies:**
  - Scope validation and segmentation controls
  - Risk assessment activities
  - Roles and processes
  - Technologies
  - Documentation

Timelines and Strategies

- **Start work on the longest projects now**
  - Some of the future-dated requirements will take major engineering efforts
  - Present your transition plan to your board or leadership
    - Service providers, this should be part of your 12.4 efforts
- **Consider your planning for your 2024 assessment**
  - If your due date is near March 31st, plan your 3.2.1 to 4.0 transition
    - Don’t play chicken with the deadline if you’re behind schedule