Back to Work: The Future of PCI

June 15, 2021

Angie Hipsher-Williams
Jonathan Sharpe
Sean McAloon
Cody Montgomery

Housekeeping

PLEASE NOTE:

- All of today's audio is being broadcast to your computer speaker.
- Please submit questions through the Q&A function on your screen. If your question is not addressed in the session, a Crowe professional will follow up with you.
- To download a copy of the presentation or access the resources connected to this session, please visit the resources icon at the bottom of your console.

CPE CREDIT

- Log in individually to the session
- Successfully complete 3 of the 4 polling questions

NO CPE CREDIT

- Failure to successfully complete 3 of the 4 polling questions
- Viewing a recording of this session (CPE is only awarded for live sessions)

CPE CERTIFICATE OF COMPLETION

- Will be available for download following the session and e-mailed within two weeks of successfully passing this program
- Upon completion of this program you will receive a post-event evaluation.

Agenda

1
Work from Home (WFH) Impacts

2
Coming Back from the Pandemic Impacts

3
Current and Future State Impact Opportunities

Learning Objectives

1
Identify areas where the pandemic may have caused issues with your PCI compliance

2
Find scope reduction opportunities within your organization’s PCI cardholder data environment (CDE)

3
Learn about different virtualization technologies and how they relate to PCI scope

4
Recognize how telephony can affect PCI scope

Presenters

Angie
Hipsher-Williams
CISA, CISM, QSA

Crowe LLP
IT Assurance Principal
+1 317 208 2430
angie.hipsher@crowe.com

Jonathan
Sharpe
CISA, CISM, QSA

Crowe LLP
IT Assurance Tech Senior Manager
+1 317 208 2433
jonathan.sharpe@crowe.com

Sean
McAloon
CISA, CISM, QSA

Crowe LLP
IT Assurance Tech Senior Manager
+1 214 777 5228
sean.mcaloon@crowe.com

Cody
Montgomery
CISA, AQSA

Crowe LLP
IT Assurance Tech Manager
+1 469 801 4355
cody.montgomery@crowe.com

PCI WFH & COVID Impacts

POLLING QUESTION

What is the state of your organization as it relates to work arrangements?

A

Our offices are fully open

B

We are taking a hybrid approach of Work From Home (WFH) and the office

C

We are completely WFH

D

Other – Please feel free to comment in the chat on how!

Cardholder Data (CHD) Acceptance (Telephony)

Protecting Telephone-Based Payment Card Data

- Updated version of the PCI Council guidance from the last published in March 2011
- Systems used to accept cardholder data (CHD), as well as those systems connected to them, are considered in-scope for PCI assessments.

WFH Impacts – Additional or new networks in scope based on call process changes

- Devices that were never in scope or considered for PCI are now in scope
    - WFH laptops that support soft phones are in-scope
- Potential systems include:
    - VoIP servers
    - Call recording systems
    - VoIP architecture (SBCs, PBX devices, etc.)
    - Session Initiation Protocol (SIP)/Session Border Control (SBC)
    - Network devices for segments these systems reside in

CHD Acceptance (Telephony)

Telephony Scope Increase Example

- **Curbside Pickup –** Point-to-point encryption (P2PE) environments
  - Implemented over the phone (VoIP) in curbside pickups in light of the pandemic
  - **Result – Scope Expansion**
    - Entire facility networks into scope

Key Takeaway

Determining all telephony-based processes, data flows, and associated systems components in use can be difficult and have an impact on scope:

- The setup, configuration, and data flows of the telephony systems will ultimately determine the scope and PCI requirement applicability.
- Telephony systems can have a large impact on scope as the data flow is usually sent across multiple segments of a corporate environment.

CHD Acceptance (Telephony)

Common strategies for Telephony scope reduction:

- Outsourcing telephony-based payment card functions to a third-party service provider or halting the direct acceptance of payment cards via telephone.
- Utilization of “Plain-Old-Telephone-System” (POTS) / traditional phone traffic or out-of-band communication
- Physical segmentation of the VoIP environment to keep all hardware in one segment and limit the telephony scope to that segment
- Dual-Tone Multi-Frequency (DTMF) Suppression or Masking
  - DTMF, familiarly known as Touch Tone, uses the telephone voice-frequency band and transmits a different tone for each associated digit.
    - On-Premises – Hardware and the associated services, processes, and CHD traffic from the VoIP environment are hosted and managed in-house.
    - Off-Premises – Hardware and the associated services, processes, and CHD traffic from the VoIP environment hosted at a third party.

CHD Acceptance

Remote Employee Laptops

- A remote workforce may mean additional workstations
  - Desktops at an office become laptops at home

Result

- New PCI requirements may be applicable. Examples include:
  - **Requirement 1.4 –** Install personal firewall software or equivalent functionality on any portable computing devices
  - **Requirement 8.3 –** Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.

P2PE Scope Increase Example

- **Curbside Pickup –** Point-to-point encryption (P2PE) environments
  - Business side rolled out additional P2PE solutions for pickup

Result

- Additional PCI scope discovered mid-assessment that IT was not aware of
- PCI compliance issues as it relates to unknown in-scope components
- Delays and request for ROC/AOC extension

PCI Assessments

PCI Council FAQs #1494 & #1496

- **1494 (May 2021) –** For personnel working from home, is the work-from-home environment considered a “sensitive area” for PCI DSS Requirement 9?
  - “No. An individual’s private work-from-home (WFH) environment is not considered a “sensitive area,” and personnel working from home are not required to meet PCI DSS Requirements 9.1.1 or 9.3 for their WFH environments.

- **1496 (May 2021) –** Are entities expected to do onsite audits of personnel work-from-home environments?
  - “No, entities are not expected to conduct onsite assessments of work-from-home (WFH) environments, as home environments are not owned or controlled by the entity.”

PCI Requirement Difficulties

Furloughed Employees

- **Requirement 6.5 –** Address common coding vulnerabilities in software-development processes as follows:
  - Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities.
- **Requirement 8.1.3 –** Immediately revoke access for any terminated users.
- **Requirement 8.1.4 –** Remove/disable inactive user accounts within 90 days.
- **Requirement 12.6.1 –** Educate personnel upon hire and at least annually.
- **Requirement 12.6.2 –** Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.

Helpdesk

- Call volumes have greatly increased, and organizations have been forced to adjust controls
  - Ex. – Password requirements
- Defining a true "business“ constraint to allow for compensating controls can be a challenge

POLLING QUESTION

What is your organization's state of PCI compliance maturity?

A

Fully Compliant – Completing Annual ROC/SAQ

B

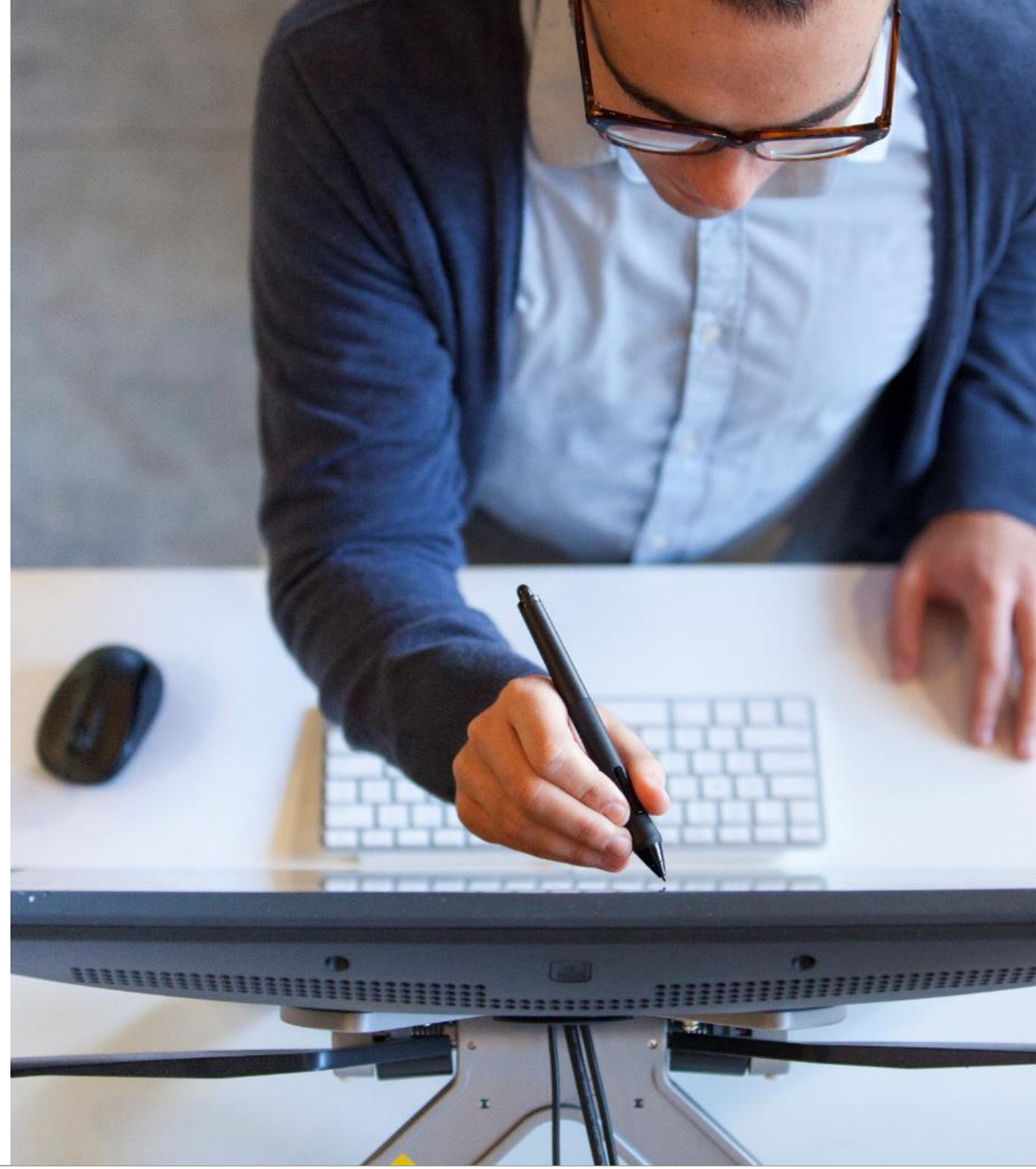
Currently Pursuing PCI Compliance

C

Have Not Begun a Road to PCI Compliance

D

I Don’t Know



Coming Back From The Pandemic

Key considerations as the world returns to work

Hybrid Work Setups

- Scope can now include both WFH and WFO setups
- Some employees will be working from both locations

Inventory Management

- Systems that have been powered off due to closures of locations may not be considered part of the CDE and therefore not in scope for the assessment. This would depend on the date of the ROC.
- Ensure you are talking with your QSA to adjust reporting dates and applicable inventory items.
- Any new systems related to new CHD processes would be added to inventory, and subsequently removed once no longer in use (if it was a temporary change, dates of changes should be recorded).

Operation of Controls

- Non-operation of controls during a period of down time may lead to non-compliance
- PCI Requirements to consider as systems come back online, and people return to work are:

1.1.7	Review firewall and router rule sets at least every six months.
3.1	A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.
6.4.6	Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.
11.1	Process to detect and identify all authorized and unauthorized wireless access points on a quarterly basis.
11.2	Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).
11.2.1, 11.2.2	Perform quarterly external and internal vulnerability scans.
11.2.3	Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.
11.3.1, 11.3.2	Perform *external and internal* penetration testing at least annually and after any significant infrastructure or application upgrade or modification.
12.6.1	Educate personnel upon hire and at least annually.
12.8.4	Monitor service providers' PCI DSS compliance status at least annually.
12.10.2	Perform an Incident Response test.

Making Changes to the CDE as Business Returns to Normal

- Turning systems back on, or adding new systems to handle increased load post-pandemic.
  - These systems will need to be patched and scanned, as they could be out of date.

- If supporting or CDE system components are added it could be considered a significant change, and PCI requirements pertaining to significant changes would be applicable: 6.4.6, 11.2, 11.3.1, 11.3.2.

- Even if these changes are temporary, they would still be determined as significant changes depending on the timing of the ROC. (A record of dates of change will be important to your independent assessor.)

POLLING QUESTION

What controls/processes were changed during the pandemic in your organization?

A

No changes, business as usual

B

Only a few changes

C

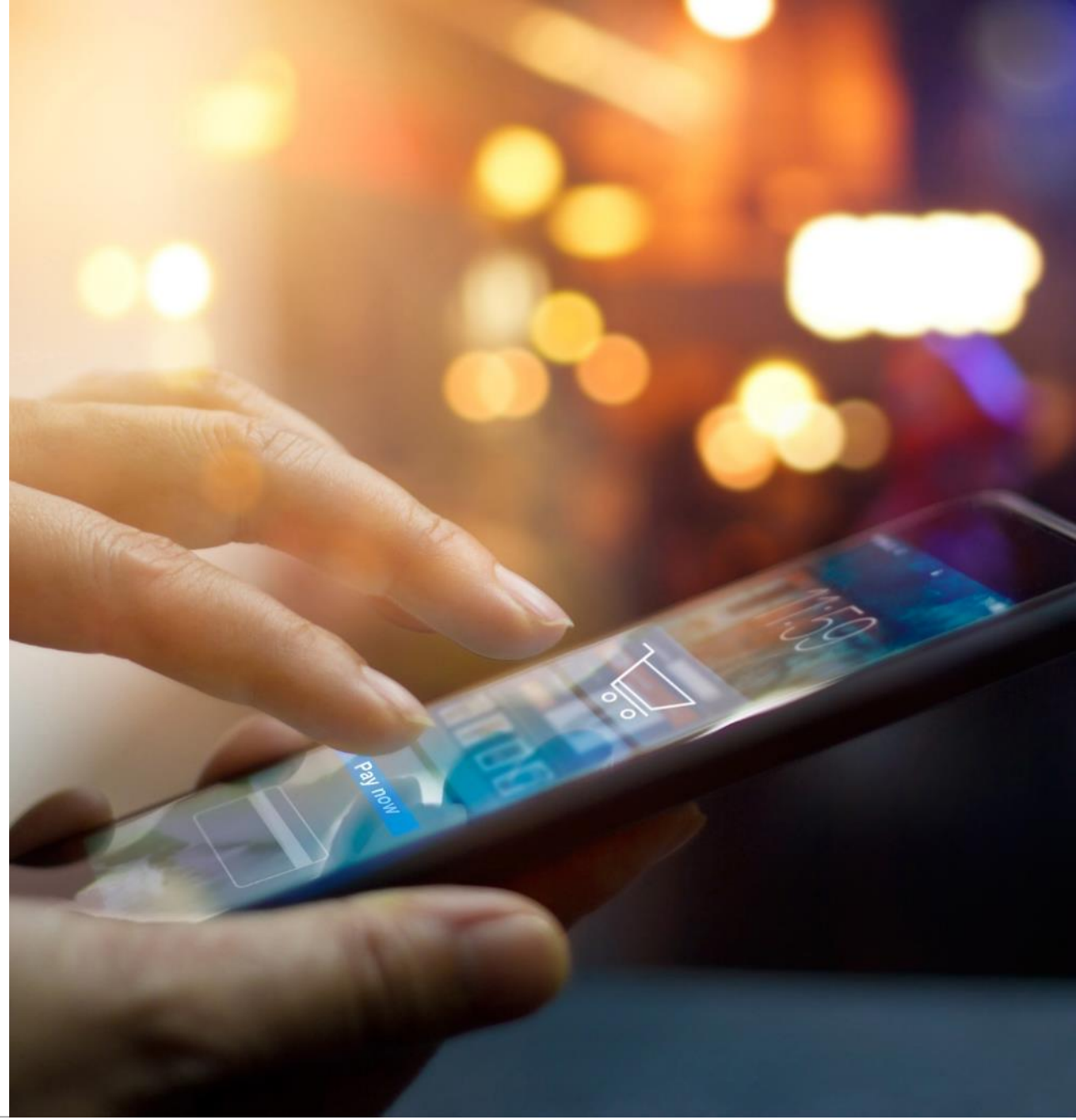
Significant changes were made to controls and processes

D

We completely changed how we operate

Continuous Compliance

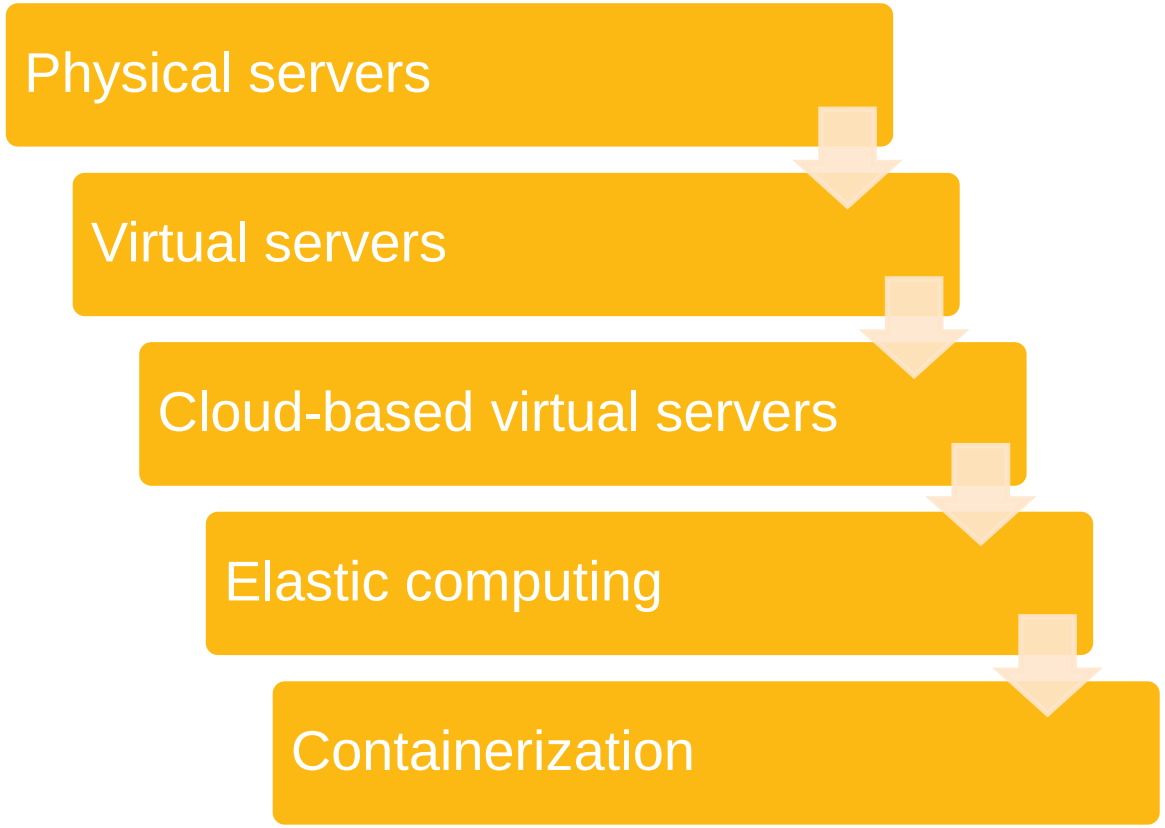
- PCI Compliance does not stop due to the pandemic or a new WFH environment, it can just change the scope of an assessment.
- There has been no change in requirements set by the council, and all requirements are still applicable and require compliance.
- Area that did change – performance of remote assessments. Speak with your QSA on the options and requirements for onsite/remote assessments.
- Requirements to “observe” certain controls did not change, only that it could be done remotely if needed.



Current & Future State Impact Opportunities

Virtualization Evolution

- Virtualization technology continues to evolve
- Interpretation and approach for these components must evolve as well to address the intent of the PCI Requirements



POLLING QUESTION

Which one of these options best represents your organization's use of virtualization and cloud infrastructure?

A

In-house physical servers and virtualization only (no cloud deployments)

B

Using cloud deployments, but static systems only (lift-and-shift)

C

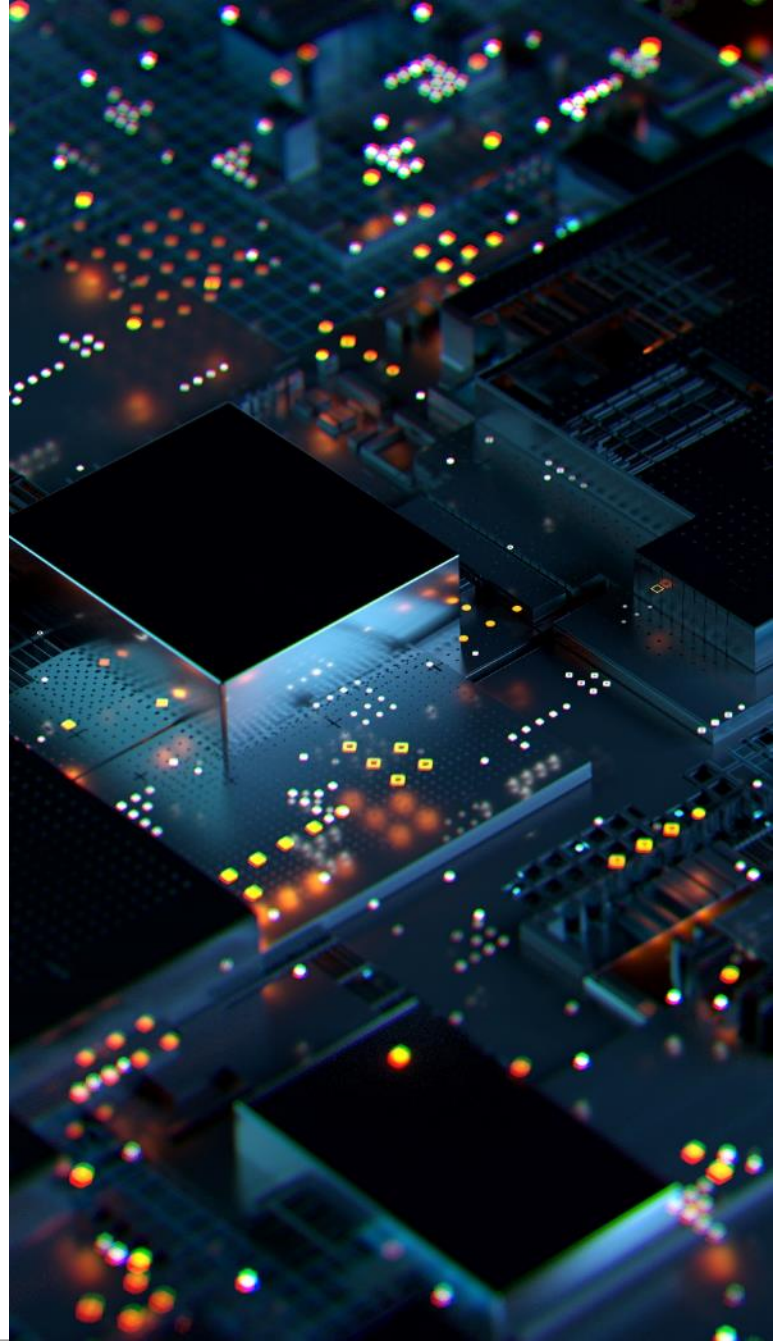
Using an elastic compute cloud deployment

D

Considering migrating to containerized applications or already using them

E

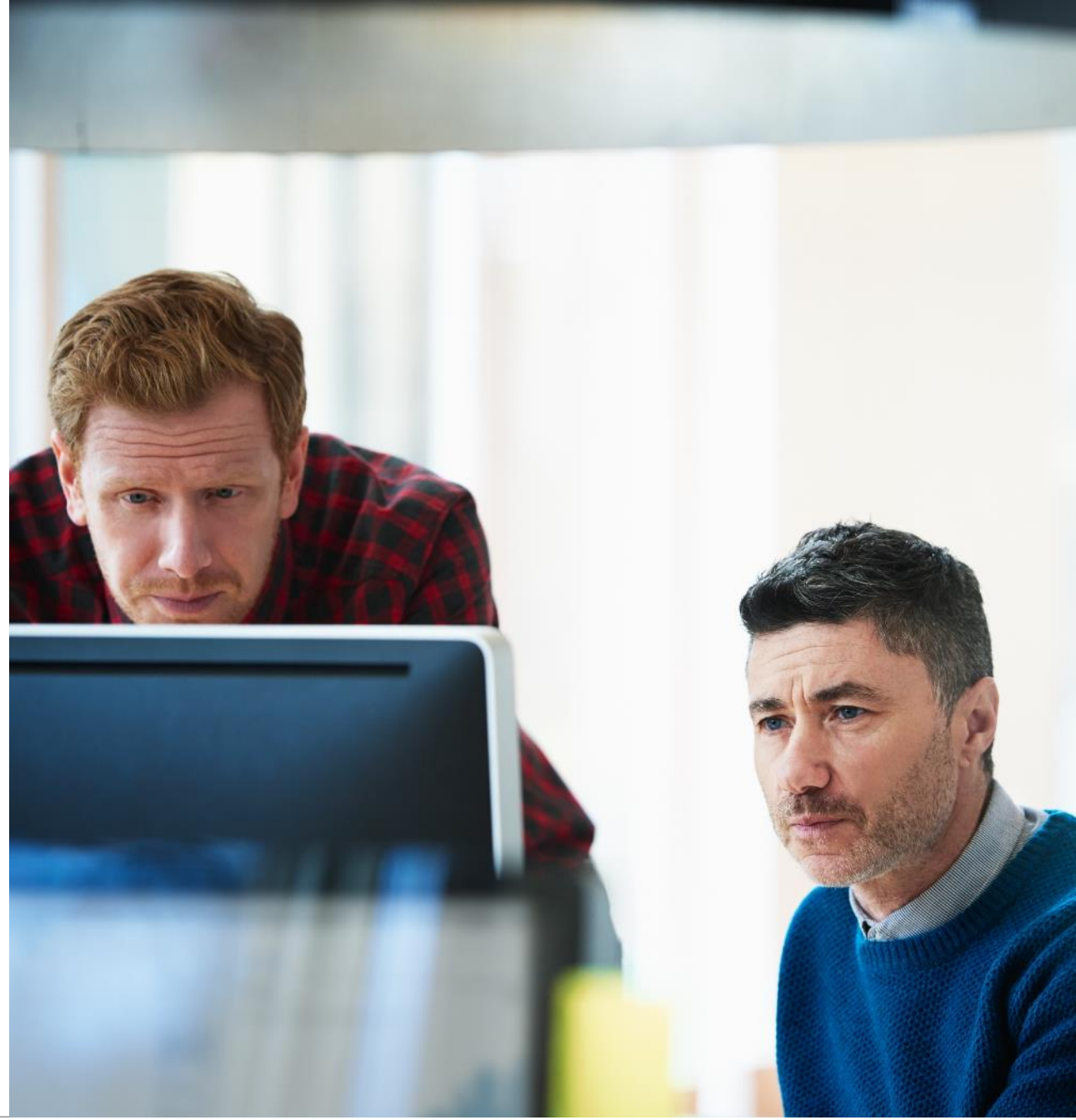
What are containers? What are you talking about?



New Points of Consideration

- These new technologies warrant a change in approach from traditional assessments
- “In-scope components” take on new meaning
- Certain PCI Requirements may not be applicable to new systems and technologies
  - For example: AV running on specific containers, container user management, etc.
- Understanding relationships and connectivity between container groups and workloads

Elastic environments and containers are designed to be lightweight, ephemeral, and scalable – how to approach?



A Shift in Approach

With the changes in technology, how has the compliance assessment approach changed?

- Changing from an assessment of the actual deployed systems to an assessment of how systems are deployed
- Build configurations
- Infrastructure as Code

Shift in Management – Configurations should be developed to meet PCI Requirements such that any new system that is automatically deployed is PCI compliant

- Applies to infrastructure (hosts/nodes) as well as actual containers
- Approaches may vary based on specific technologies and components

A Shift in Approach

What?

- “Does the sampled server receive patches monthly?”
- “Show that the sampled server sends logs to a centralized location.”
- “What user accounts exist on the system?”

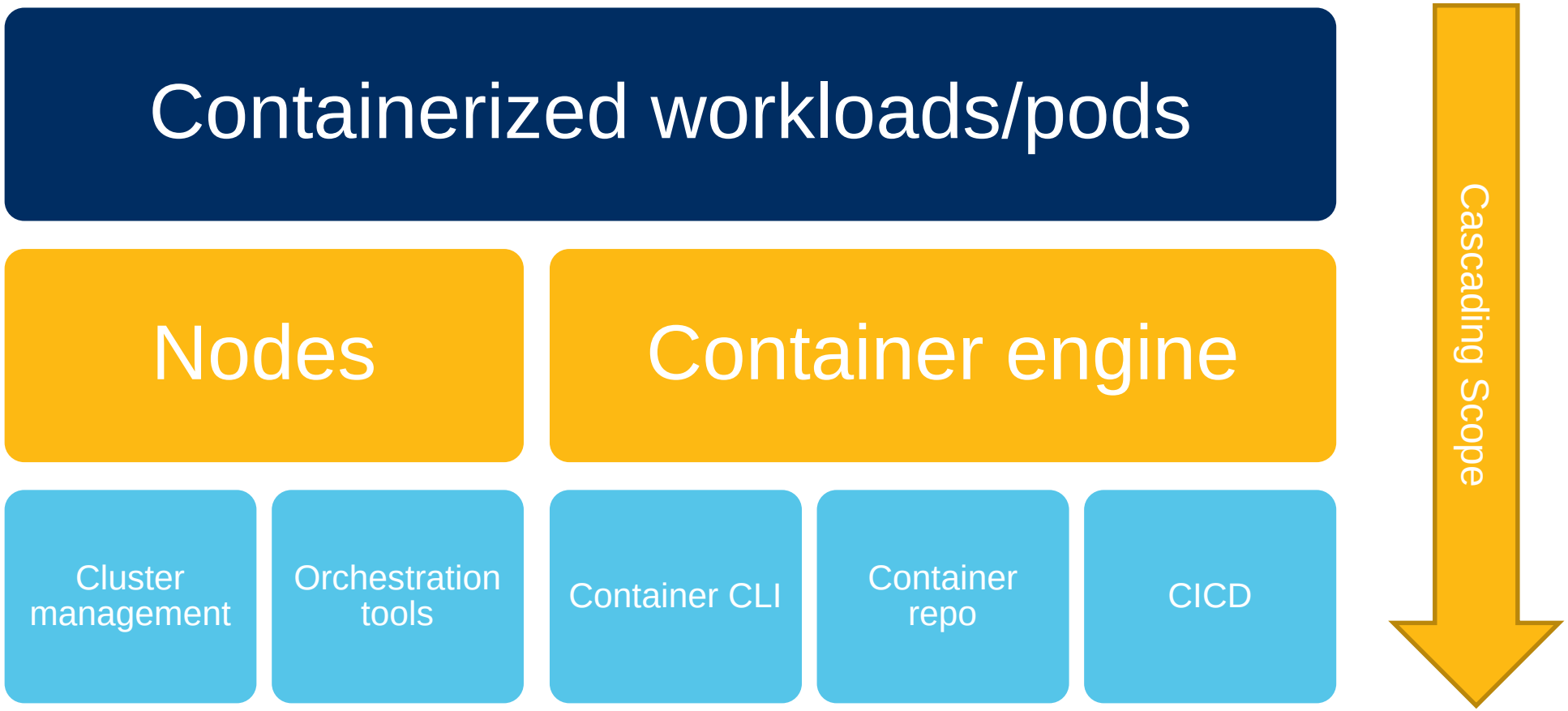
How?

- “How are instances deployed with the most up-to-date patches?”
- “How are new servers configured to send logs to a centralized location?”
- “How are user accounts added to the configuration, and who can manage the configuration?”

Containerization Considerations

- Scope impacts of containers – what to consider?
  - Running containers
  - Nodes
  - Container engine
  - Container registry
  - Data storage locations
  - Orchestration tools
  - Networking
  - Deployment pipeline
  - Logging and other monitoring tools

Containerization Considerations – Scoping



Containerization Considerations

- Container workloads must be isolated to maintain segmentation – PCI-relevant workloads cause all supporting elements to be in scope
- Host/node-level requirements are consistent with traditional assessments
- Limiting access to actual containers, deployment processes, orchestration tools, and container CLIs
- Logging and monitoring at the container and host levels
- Vulnerability management and emerging threats
  - Threats exist both at the container level and the host level
  - Assess against production instances and container registries
  - Siloscape malware

"Segmentation on a cloud-computing infrastructure must provide a level of isolation equivalent to that achievable through physical network separation."

What Should You Consider?

- Your QSA can help define what warrants consideration in relation to containerization or other cloud deployments
- Asking questions early and often to avoid scope surprises:
  - How will a container deployment impact my CDE?
  - What additional security elements need to be considered?
  - How will existing processes need to be modified to meet the intent of the PCI Requirements?

- Container security and compliance guidance:
  - PCI SSC Cloud Computing Guidelines
  - NIST SP 800-190
  - ISACA Application Containers Audit Program
  - SANS Controls

Maintaining An Inventory

- The nature of cloud environments increases the difficulty of maintaining an accurate list of in-scope components
- Scalability and elasticity changes the number of components continuously
- Inventory itself should focus on:
  - Container repository, rather than actual running workloads
  - Running hosts/nodes
  - Base images and Infrastructure as Code

Focus on processes and controls for how the inventory is maintained

Questions?

Thank you

Angie Hipsher-Williams
IT Assurance Principal
+1 317 208 2430
angie.hipsher@crowe.com

Jonathan Sharpe
IT Assurance Tech Senior Manager
+1 317 208 2433
jonathan.sharpe@crowe.com

Sean McAloon
IT Assurance Tech Senior Manager
+1 214 777 5228
sean.mcaloon@crowe.com

Cody Montgomery
IT Assurance Tech Manager
+1 469 801 4355
cody.montgomery@crowe.com