
PCi
Security
Standards Council
®

PCI Security Standards Council

Managing Data and Data Center Assessments In Today's Remote World

Today's on-site assessments are not the old brick and mortar assessment world of assessment activities!

PCI Security Standards Council

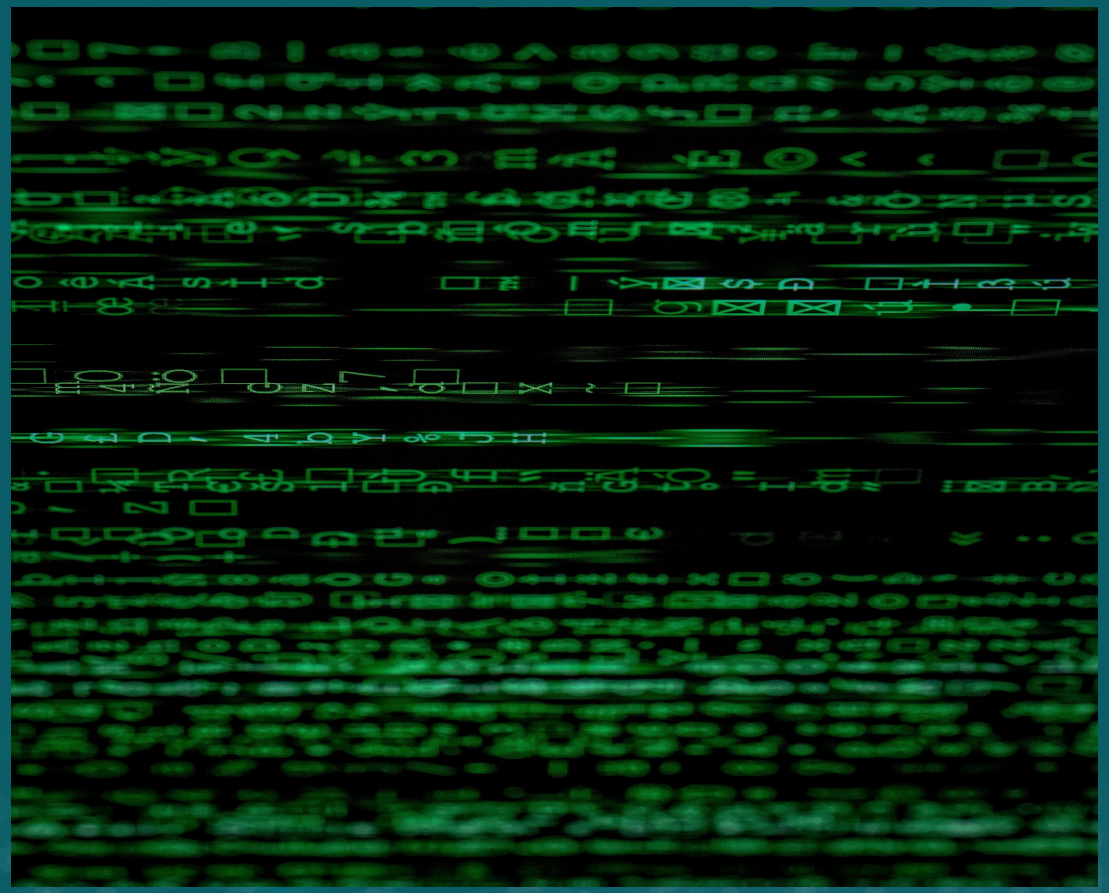
Howard Glavin

EVP K3DES, LLC
QSA, PCIP, CISM, CRISC, CDPSE, ISO 27001/IEE Senior Lead Auditor

K3DES

Setting the Stage

Differences Between Owned Data Centers and Colocations



Types of data centers

- You own the data center
- You lease the data center, and you manage (Colocation specifically dedicated to your needs)
- You use a colocation shared with others on dedicated space and devices to you
- You are using a cloud-based service with dedicated devices
- You are using a cloud-based multi-tenant service

PCI Security Standards Council®

What You See is What You Have!

Only if You Observe Everything – Blinders Do Not Serve You Well

Observations are the key to this part of the assessments

- Look for what is to your left and right
- Look up
- Look down
- Open doors
- Ask to see storage areas and loading docks
- Trash collection areas
  - All the above can be completed in a remote assessment by having the camera you are seeing move to your request

PCI Security Standards Council®

Data in the Data Centers

Hide and Seek! The media is everywhere

Data in data centers…what a strange concept

- Data is on standard hard drives
- Data is on solid state drives
- Data is on tapes
- Data is on CDs and other removable media
  - All the above data may be on functioning or non-functioning devices
- Being able to maintain an inventory of all data locations is difficult but doable and verifiable
- Inventory equates to accountability

PCI Security Standards Council®

Physical On-Site Check Lists and Processes

Myopic vision will not serve you well

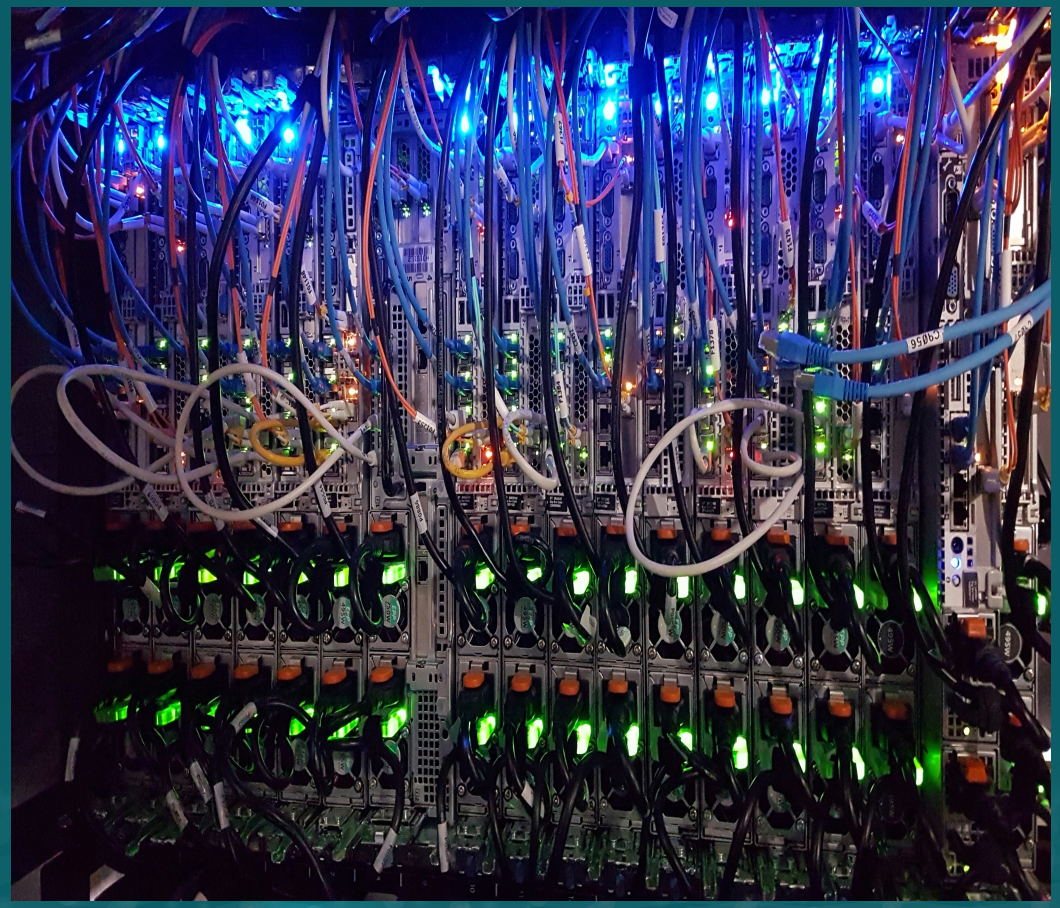
When everything looks alike, challenge your viewing

- Yes, the view is shoes (so to speak)
  - They differ in pattern, style, color, etc.
- FYI – What is the wire hanging down doing? Did you only see the shoes?
- Ensure what you are observing is actually "observed"
- Remote is doable but requires due diligence

PCI Security Standards Council

Pitfalls in Assessments for These Types of Facilities

Real World Part 1



On-site or remote; do you know what you are looking at?

- Look at the image to the left
  - What is it?
  - Is it upside down?
  - What are you seeing?
- It actually happened example:

  In the loading dock area, pallets of devices ready for pick up for shipment to South America. These were sold as surplus. The data was never wiped.
  - Processes MUST be followed

PCI Security Standards Council

Pitfalls – On-site

Real World Part 2

The maze of items in the physical on-site can be interesting

- Example – colocation with dedicated racks in a cage dedicated to the customer
  - Cage key get charged out at security office
  - Rack keys get charged out at the security office
  - No logs of who received the keys
  - No logs of when the keys were returned
  - No validation the keys did not leave the premise
  - No cameras for cage or rack
  - Use a check list to be sure to cover all items

PCI Security Standards Council

Pitfalls – On-Site and Remote for Devices Controls

Real World Part 3

Service providers in data center

It actually happened example:

- Major health care company in the US had a third-party doing services in dedicated data center delivering new equipment
  - Equipment delivered
  - Equipment to be removed was removed
  - Several servers with PII – PCI data also removed from racks
    - Loss of live data not realized for several days due to cluster use and miss by admins on part of the cluster not responding
    - Can you say breach!
  - The owner must protect the assets to prevent loss

PCI Security Standards Council

Remote Assessments for All Forms of Data Centers Less Cloud

Proven processes are the key drivers

You are only seeing what they choose to show you via video. You only see a very narrow view of the world as shown by your GUIDE

- All the unlocked doors, etc., are not part of the show-and-tell via the video
- It actually happened example:
  - Old dial-up device found attached to core switch
  - Modems found in many racks
  - Portable hard drives found attached to servers
- Be sure you ask to see everything you would view in person

PCI Security Standards Council®

Remote Assessment Colocations

Colocations and the use of phones and cameras in the raised floor areas

If prohibited, completing a remote assessment can pose challenges.

- A Solution if the Data Center is not PCI Compliant, is to work with the vendor to conduct the assessment remotely with their staffing, utilizing their phone, laptop or tablet to show the items that are required to be validated.
- If video is not possible then ask for photos of the various items, you are attempting to validate.
  - Rack content front and back
  - Surplus and spare equipment area
  - Security controls to the Facility, Room, Rack, or Cage

PCI Security Standards Council

Ping Power and Pipe With or Without Power Cycle

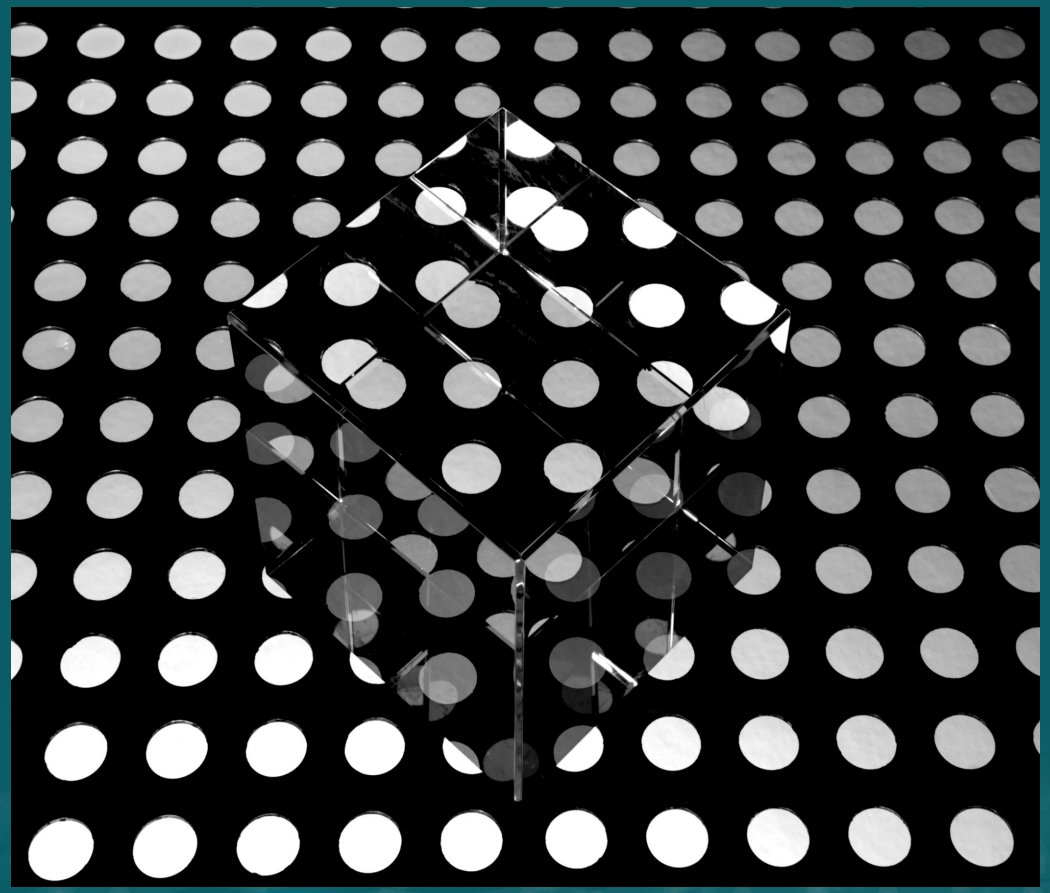
The arguable best world for you in a colocation

- The colocation owns and manages the building
- You own and manage your rooms, cages, racks, and devices
  - The full liability and responsibilities of management of the device and related data is squarely on your shoulders
  - Potential issues; the colocation manages the keys to the rooms, cages, and racks
    - Do they access your private space
    - How are you managing the keys they hold in a key safe – storage container?

PCI Security Standards Council®

Colocations with Full Operation of Your Devices as Your Support Staff – Non-PCI Compliant

Contracts and SLAs are the drivers to this success and compliance



Contracted to outsource the full support and facility activities to them

- What SLAs did you set?
- What types of screening did you require for the staff supporting your needs?
- What training did the staff receive for PCI needs?
- What change management system are they using to support your needs?

PCI Security Standards Council®

The Cloud and Vulnerability Management – Penetration Testing

Vulnerability Management and Penetration Testing Issues

The joys of the unknown

- Scanning is generally doable with some concessions and different tool sets
- Penetration testing is generally is workable for your devices
  - If permitted testing is limited to your containers
  - How do you get the full "Big Picture" to test
    - All devices in your stream
    - What does the provider test?
    - What test results are shared with you?
      - Contracts and SLAs articulate these provided evidence needs

PCI Security Standards Council

The Cloud Part

Cloud Providers Have Great Advantages if PCI Compliant

- Cloud Providers who met PCI DSS Compliance have:
  - Excellent security tools to help reduce your needs
  - Scanning tool for containers that do a much better job than the conventional tools
  - Are staffed and managed by very competent staff that see many exposures that you would not see and report back to you
- If the provider has their own AoC and Responsibility Matrix, this could meet your compliance needs based on the Matrix

PCI Security Standards Council®

Conclusions

Can Remote Assessments of Data Centers work?

- Remote Assessments are possible in all cases
  - The end results may vary based on how open the locations are with sharing data
  - Compliance needs specified in advance to the remote visit generally gain the camera needs you require
- Data in the data centers
  - Is in servers
  - Is in loose drives, tapes, removable media
  - Data leaks out of data centers when it is removed for the servers or SEIM devices
    - Don’t forget to look for these devices remotely – ASK and you will receive

PCI Security Standards Council®

Questions

Email: Howard.Glavin@K3DES.com
Mobile: +1 904.631.9204
Come see me at Booth 25

THANK YOU!


PCi
Security
Standards Council
®