

How To Manage Scope Even When It's Always Changing

Peggy Nolan, CEO
Payment Card Assessments, LLC



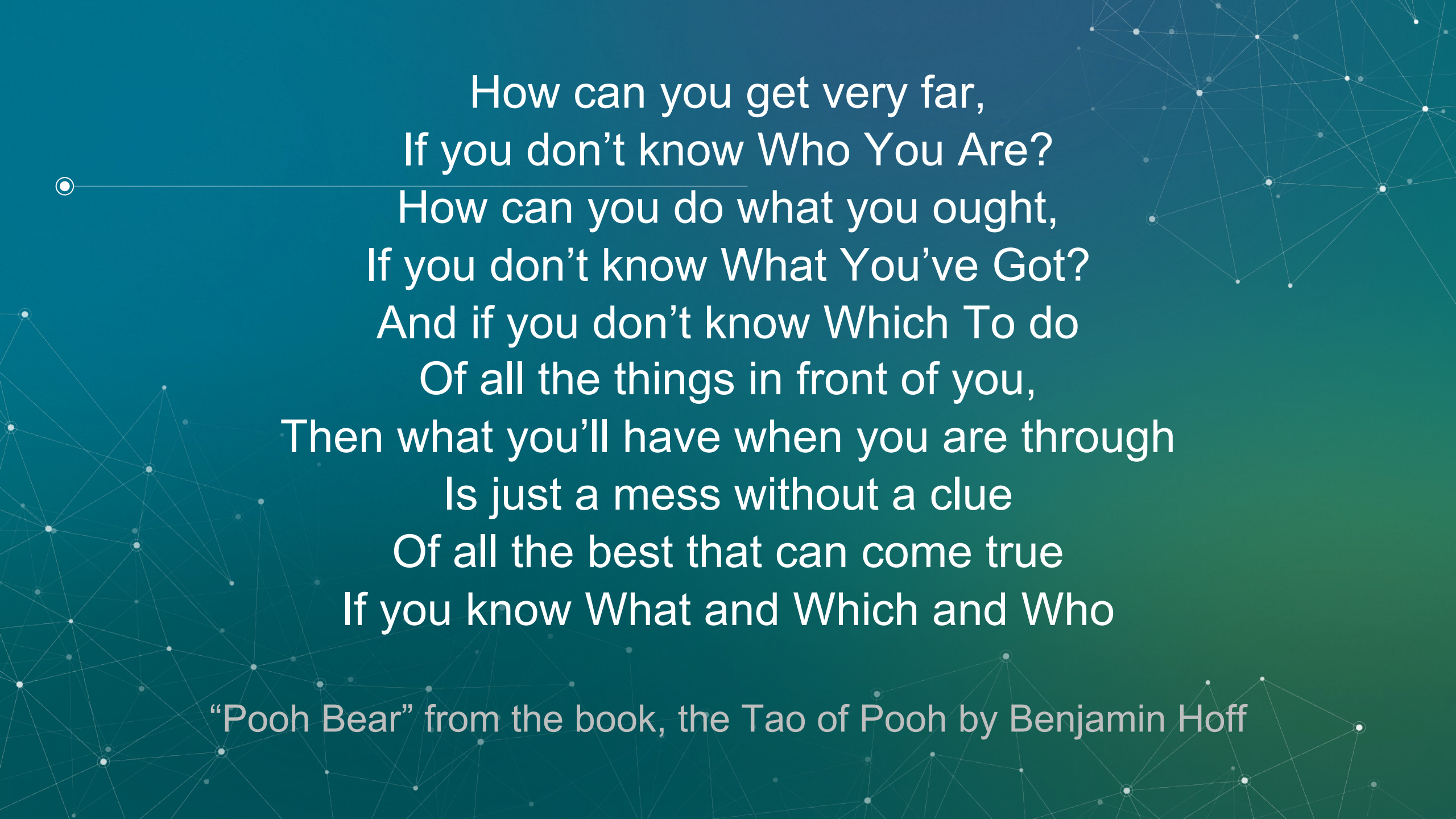
Introduction



It's 2 AM...

Do you know where your cardholder data is?

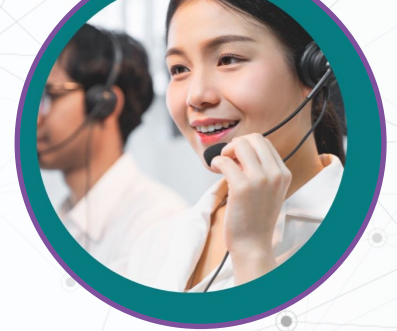




How can you get very far,
If you don't know Who You Are?
How can you do what you ought,
If you don't know What You've Got?
And if you don't know Which To do
Of all the things in front of you,
Then what you'll have when you are through
Is just a mess without a clue
Of all the best that can come true
If you know What and Which and Who

“Pooh Bear” from the book, the Tao of Pooh by Benjamin Hoff

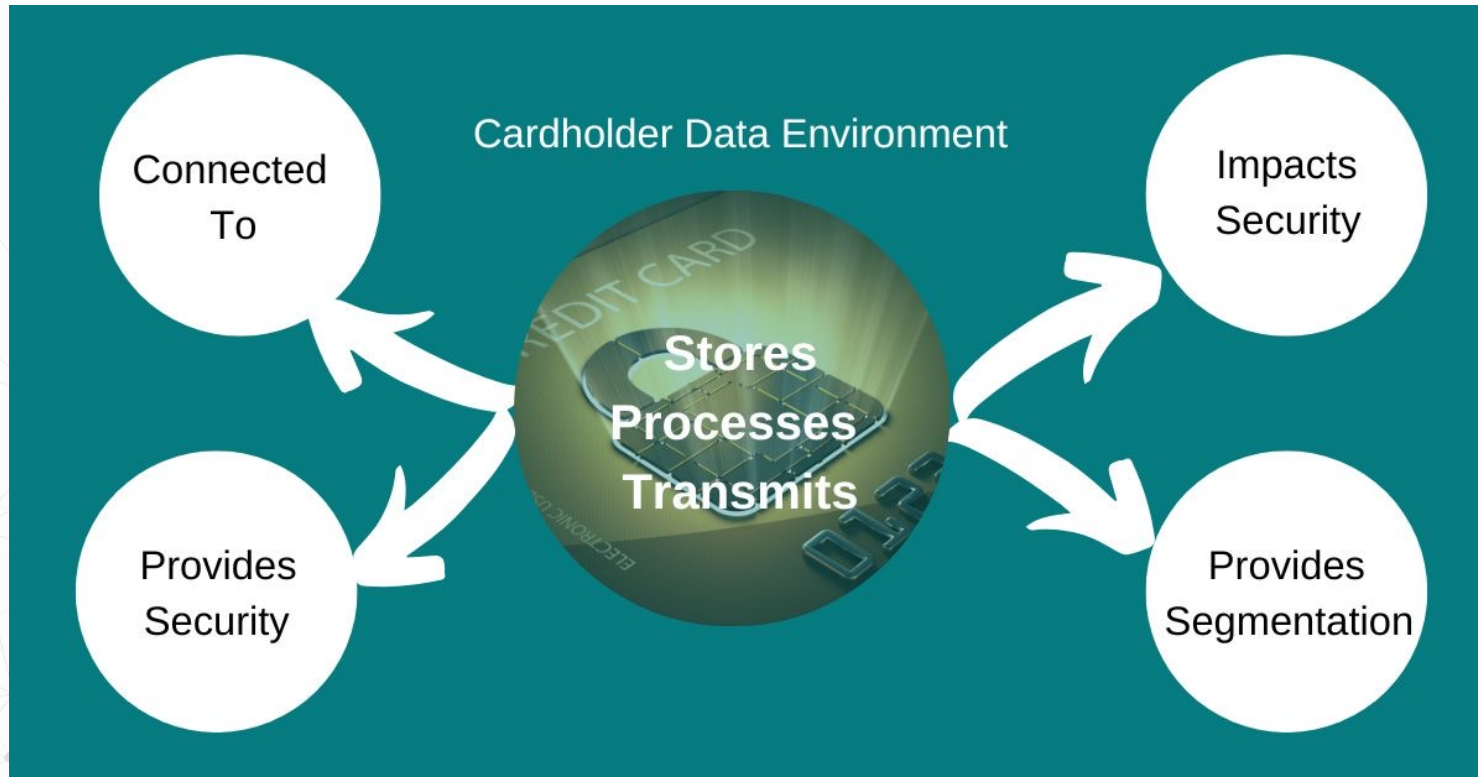
How Can You Get Very Far If You Don't Know What's In Scope?



People

Processes

Technologies



Understanding Scope is Fundamental to a Successful PCI DSS Compliance Program



- Continuous Compliance
- Report on Compliance
- Self Assessments



“How can you do what you ought if you don’t know what you’ve got?”

Six Simple Steps To Manage Scope



Step 1



Reduce Scope Whenever & Wherever Possible



Step 2

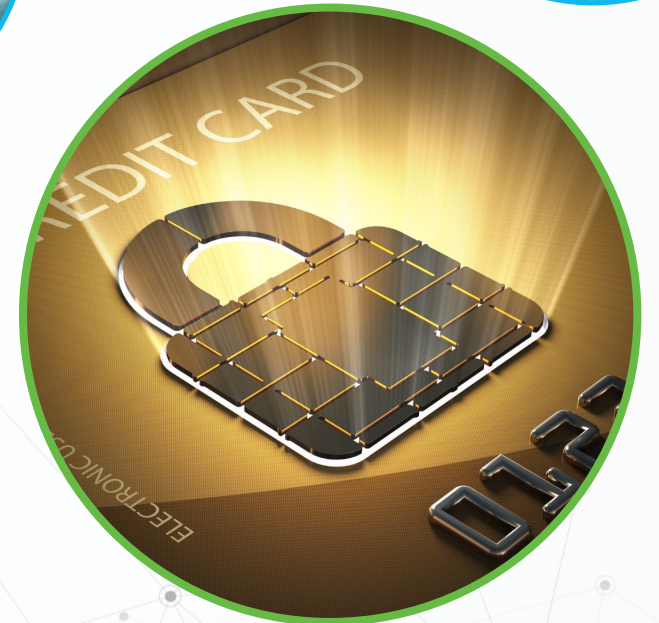
Follow the Money



Step 3



Keep Following the Money



Step 4



Create Formal Processes to Manage Scope



Step 4



Create Formal Processes to Manage Scope



Step 4



Create Formal Processes to Manage Scope



Step 5



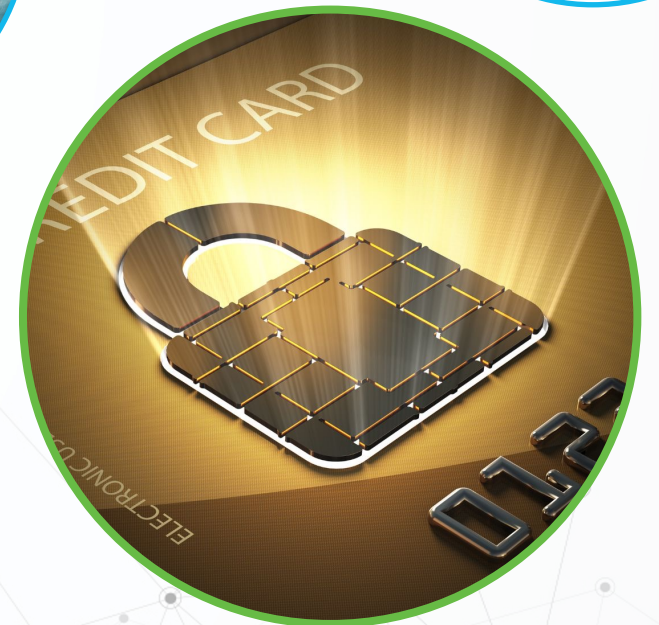
Automate Your Formal Processes



Step 6



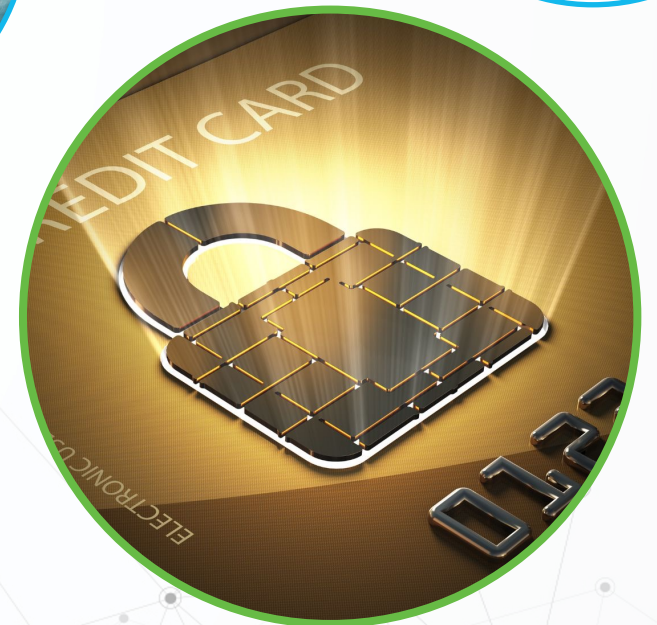
Continuously Validate Your Scope



Step 6



Continuously Validate Your Scope



Do You Know What & Which & Who?



Have you reduced scope wherever possible?

Do you have processes in place to manage changes to your cardholder data environment whether it's people, processes or technology?

Do you know who your subject matter experts and control owners are?

Last Question...

If I asked you for your in-scope inventory, would you feel confident in its accuracy?

Thank you!

Website: <https://paymentcardassessments.com>

LinkedIn: <https://www.linkedin.com/in/peggynolan/>



Payment Card Assessments, LLC

