

ARCHITECTURE BEFORE CHECKLIST

START WITH THE ASSET

A requirement becomes understandable when you can name what it protects, where it operates, and which relationships make it relevant.

SCOTT NORTON / PCI DSS QSA | JOHANSON GROUP, LLP

01

**A CHECKLIST BEGINS WITH A REQUIREMENT.
AN ENVIRONMENT BEGINS WITH ASSETS AND
RELATIONSHIPS.**

THE SAME RULE, ACCOUNT, SERVER, OR SERVICE CAN MEAN SOMETHING DIFFERENT DEPENDING ON WHAT IT CAN AFFECT.

03

**INVENTORIES MATTER. ROWS ALONE HIDE
THE EDGES THAT EXPLAIN IMPACT.**

04

**ASSETS USE SERVICES. IDENTITIES
ADMINISTER SYSTEMS. PROVIDERS
PERFORM ACTIVITIES. EVIDENCE SUPPORTS
CLAIMS.**

05

**ASK WHY THE REQUIREMENT EXISTS HERE
BEFORE ASKING FOR THE EVIDENCE PACKAGE.**

**TRACE ONE PATH: SOURCE, DESTINATION,
PURPOSE, OWNER, APPROVAL,
CONFIGURATION, EVIDENCE, CHANGE
TRIGGER.**

SEPARATE OBSERVED FACTS, INHERITED ASSUMPTIONS, AND SCOPE OR CONTROL CONCLUSIONS.

08

**START WITH THE ASSET. FOLLOW THE
RELATIONSHIPS.**

ONE MOVE TO MAKE NOW

Pick one important asset and trace one real connection or administrative workflow through its purpose, owner, approval, configuration, evidence, and change trigger.

MY PRACTITIONER POSITION / SCOTT NORTON