

FIRST ASSESSMENT

THE VIRGIN ASSESSED ENTITY

A first-time assessed entity does not need condescension. It needs a truthful map, a shared vocabulary, and permission to discover what the questionnaire never taught it to ask.

SCOTT NORTON / PCI DSS QSA | JOHANSON GROUP, LLP

01

A FIRST-TIME ASSESSED ENTITY MAY HAVE CAPABLE SECURITY PRACTICES AND VERY LITTLE ASSESSMENT CONNECTIVE TISSUE.

START WITH PAYMENT CHANNELS, DATA FLOWS, SYSTEMS, IDENTITIES, PROVIDERS, AND BUSINESS PROCESSES - NOT A FOLDER OF EVIDENCE REQUESTS.

03

TRANSLATE ASSESSMENT VOCABULARY INTO THE ENTITY'S OPERATING LANGUAGE AND TRANSLATE THE ENVIRONMENT BACK TO THE ASSESSOR.

04

**THE FIRST DIAGRAM, INVENTORY, MATRIX,
AND EVIDENCE LIST ARE WORKING
HYPOTHESES.**

05

RECORD DISCOVERIES WITHOUT TURNING THEM INTO BLAME. A MISSING DEPENDENCY IS USEFUL ONCE IT BECOMES VISIBLE AND OWNED.

06

**EVERY MANUAL EVIDENCE HUNT SHOULD
LEAVE BEHIND A REPEATABLE SOURCE,
QUERY, OWNER, CADENCE, AND
INTERPRETATION PATH.**

07

**THE FIRST ASSESSMENT SHOULD PRODUCE A
LEARNING SYSTEM, NOT ONLY A REPORT.**

08

BUILD THE SECOND ASSESSMENT CORRECTLY WHILE COMPLETING THE FIRST.

ONE MOVE TO MAKE NOW

Create a first-assessment discovery ledger with five columns: what we believed, what we observed, why it differed, who owns the correction, and what becomes repeatable next cycle.