

W/ CENTERPIECE CONFERENCE SEGMENT

THE DIAMOND FULCRUM OF PCI DSS

Keeping scope, applicability, responsibility, and evidence
in formation

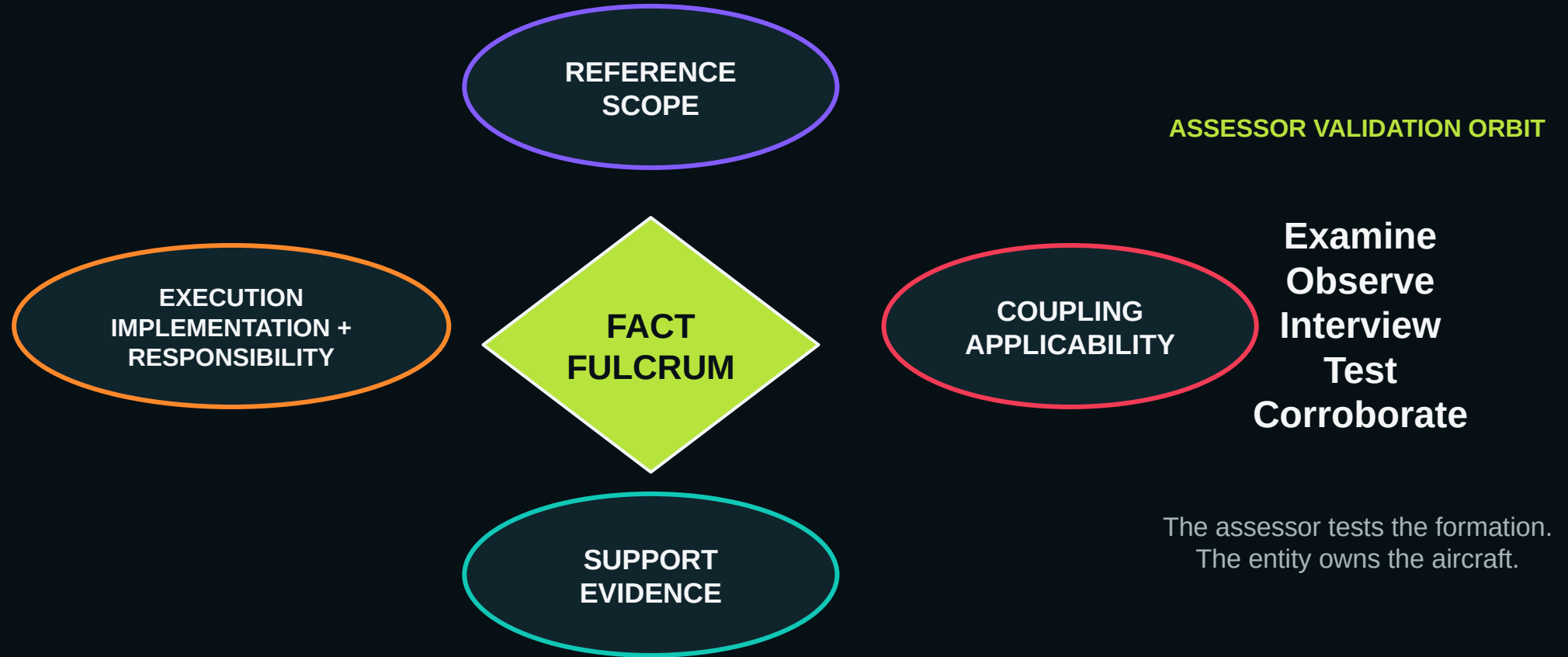
SCOTT NORTON / PCI DSS QSA / JOHANSON GROUP, LLP

FORMATION DRIFT

The inventory, diagram, provider packet, test population, and evidence repository can each look reasonable while describing different environments.

FOUR CLAIM POSITIONS

Scope. Applicability. Implementation and Responsibility. Evidence.



THE FACT FULCRUM

Assets, services, data flows, identities, locations, providers, responsibilities, configurations, occurrences, and changes form the shared reference.



SCOPE AS REFERENCE

Which people, processes, technologies, locations, data, and relationships does the assessment represent?



APPLICABILITY AS COUPLING

Which obligation connects to which subject, predicate, tested fact, authority, response, and reopening trigger?

IMPLEMENTATION AND RESPONSIBILITY

Who configures, operates, monitors, reviews, responds, changes, preserves, and proves?



EVIDENCE AS SUPPORT

What supports this claim for the correct subject, population, period, and procedure?

SIGNIFICANT CHANGE MANEUVER

**Change the fact. Reopen the claims. Move the consumers.
Validate the new formation.**



THE ASSESSOR VALIDATION ORBIT

The assessor tests the formation. The entity owns the aircraft.



FORMATION CHECK

Choose one changed payment fact. Identify every position and downstream artifact that must move.



KEEP THE CLAIMS IN FORMATION

Find the changed fact. Map the affected claims. Explain ownership. Reduce unsupported assertions. Prove what remains.
