

GOVERNANCE SURVIVES OUTSOURCING

AN AOC DOES NOT OUTSOURCE GOVERNANCE

Provider assurance matters. The customer still needs to understand the service, the allocation of responsibility, and the handoffs where assumptions accumulate.

SCOTT NORTON / PCI DSS QSA | JOHANSON GROUP, LLP

01

**A PROVIDER CAN OPERATE THE CONTROL. THE
RELATIONSHIP STILL NEEDS GOVERNANCE.**

02

AN AOC IS VALUABLE EVIDENCE ABOUT THE PROVIDER AND ASSESSED SERVICES IT DESCRIBES.

03

**IT CANNOT KNOW EVERY CUSTOMER
SERVICE TIER, CONFIGURATION, FEATURE,
ACCESS PATH, OR HANDOFF.**

**START WITH THE EXACT SERVICE BEING
CONSUMED AND WHERE IT SITS IN THE
ARCHITECTURE.**

05

SEPARATE PROVIDER-PERFORMED, CUSTOMER-PERFORMED, AND SHARED ACTIVITIES.

06

FOR EACH ACTIVITY: WHO ACTS, WHAT EVIDENCE EXISTS, HOW FAILURE SURFACES, WHO DECIDES NEXT.

07

**SHARED RESPONSIBILITY IS A NAMED
HANDOFF, NOT A GENERAL STATEMENT THAT
BOTH PARTIES CARE.**

08

AN AOC DOES NOT OUTSOURCE GOVERNANCE.

ONE MOVE TO MAKE NOW

Choose one critical provider service and map five relied-upon activities to the provider action, customer action, evidence, failure signal, and named decision owner.

MY PRACTITIONER POSITION / SCOTT NORTON