Optimizing Third-Party Risk Management with Automation

Siobhan Hunter

Director, IT Governance, Risk and Compliance

Blue Cross NC

The Road to Winning the CSO50

Third Party Risk Management Revamp

Presenter: Siobhan Hunter, Director, IT Governance, Risk and Compliance

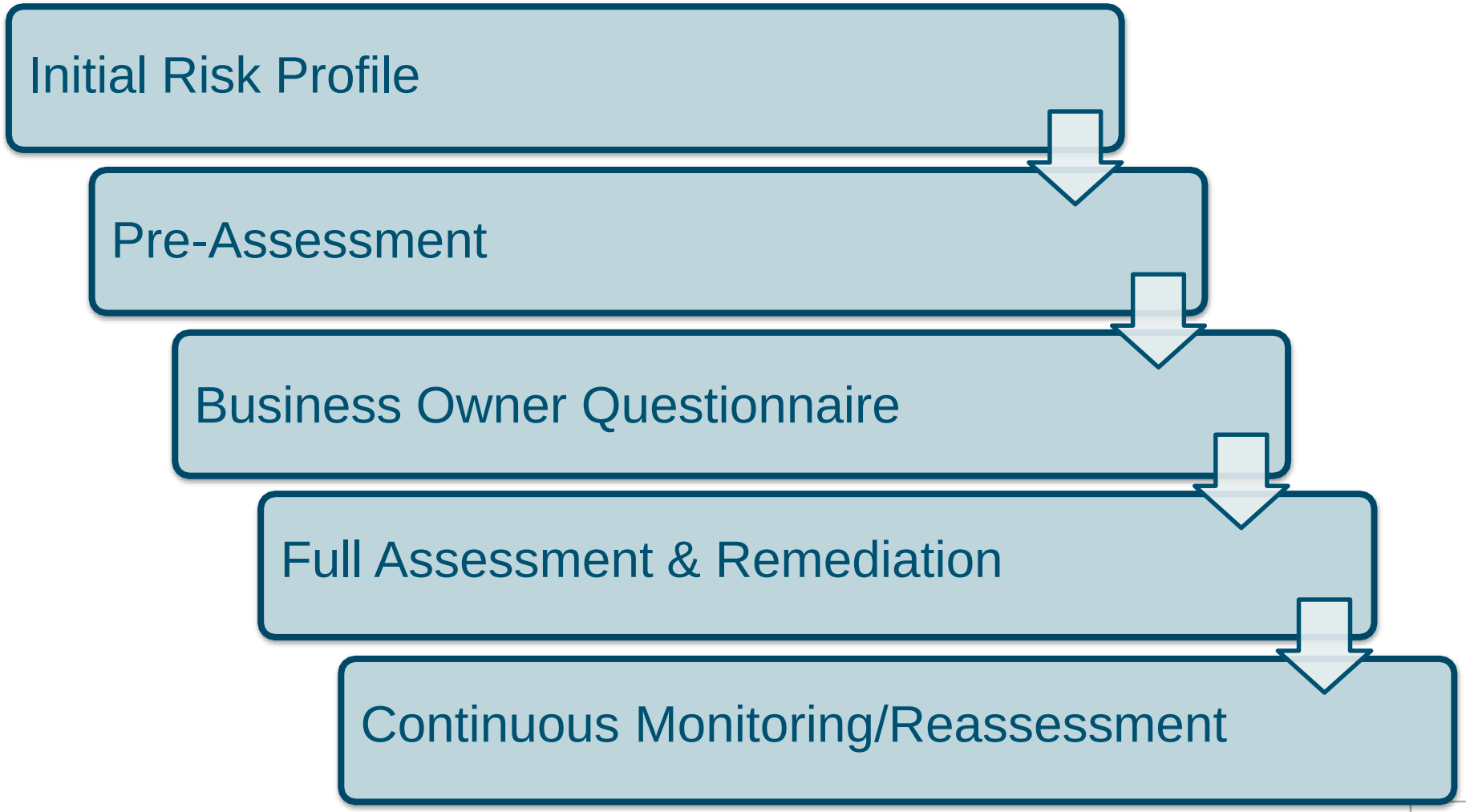
BlueCross BlueShield of North Carolina

OPPORTUNITIES WITH EXISTING SECURITY ASSESSMENT PROCESS

+ Tier 1 Enterprise Security Risk
+ No variation between RFX/POC and full security assessment
    - One size fits all
+ Inconsistent understanding of how business is leveraging the 3rd party as well as changes to the engagement.
+ Lack of follow through with 3rd parties on security remediation actions
+ Lack of defined re-assessment cadence
+ Lack of ongoing monitoring for major 3rd party changes
+ Confusion/lack of communication between internal stakeholders- i.e. Vendor Managment, Internal Audit

WENT TO THE DRAWING BOARD

NEW THIRD PARTY RISK MANAGEMENT PROGRAM



PARTNERING WITH A MANAGED SERVICE PROVIDER

+ Opportunity to move from project managers to risk advisors for the business owners
+ Complemented our new process
  - Offered:
    - Timely pre-assessments
    - Shorter security assessment process with appropriate assurances
    - Remediation strategy and tracking to hold vendors accountable
+ Highly collaborative
  - Integrated with GRC platform
  - Integral part of TPRM maturity
+ Solely operates in the healthcare vendor assessment space

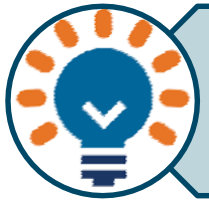
SUMMARY OF IMPROVEMENTS (RESULTS/WINS)

+ Visibility into the inherent risk of vendor population
+ Increased Collaboration with Stakeholder enabling improved decision making via early involvement in procurement process
    - Third Party Governance Meetings
+ Vendors tiered based on security risk profile (no one size fits all)
+ Documented remediation of 3rd party risk including tracking within the Risk Register
+ Reassessment cadence to track improvement of security posture overtime
+ Comprehensive Assessment process which is more efficient and accurate

LESSONS LEARNED

Data Integrity

Vendor Governance



Continuous Improvement

Communication