PONDURANCE

VENDOR SECURITY RISK ASSESSMENT PROGRAM

VISION, PROCESS, AND METHODS

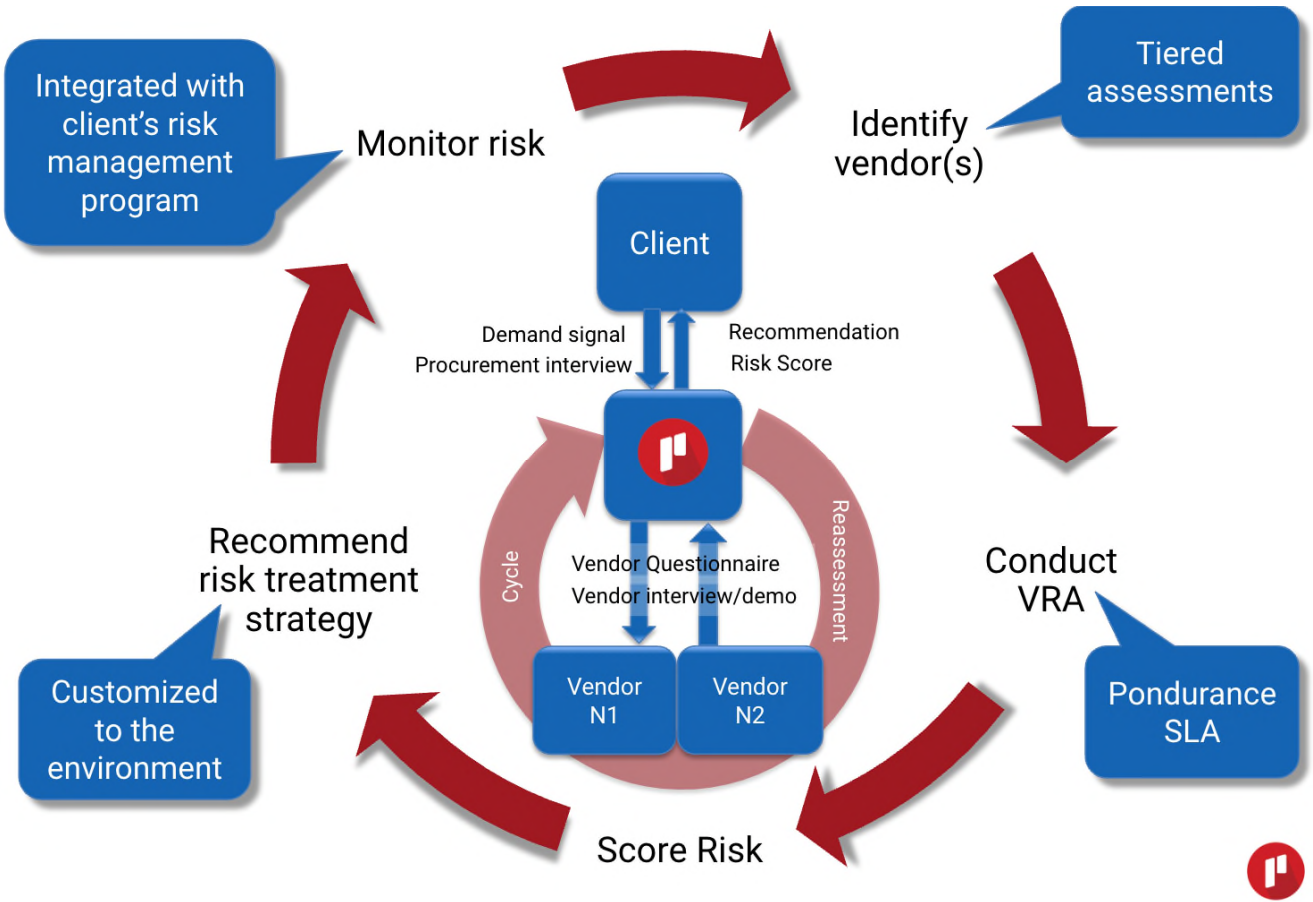
Nicole Sigler, QSA, CISA, CISM, CMMC RP
Senior Security Consultant

VISION

- Target market: Regulated industries and their suppliers processing or storing in the cloud or adopting new technologies (applications).
- Based on the NIST CSF.
- Build a database of provider security risk assessments.
- Recommendations tailored to client's risk environment.
- Failure to assess third-party risks exposes an organization to supply chain attacks, data breaches, and reputational damage.

PONDURANCE

PROCESS



PONDURANCE

METHODS

- Vendor risk assessment procedure
- Information intake form
- Vendor questionnaire(s) and interviews
- Risk scoring methodology
- Tailored recommendations

PONDURANCE

PROCEDURE – TIERED ASSESSMENT

- A risk-based approach to vendor assessment activity will be taken considering certain criterion. An assessment of vendor controls will be performed if the vendor has not been assessed within the last year AND meets one of the following criteria, which has been incorporated into the security assessment:
    - Has access to personally identifiable information (PII), protected health information (PHI), or the cardholder data environment (CDE), or (fill in the blank) – a full security assessment will be completed
    - Does not have access to PII or (fill in the blank), but is critical to client's business operations – a partial assessment will be completed
    - Has connectivity to or access into the client's network
- The consultant assigned to the assessment reserves the right to make a decision regarding the extent of assessment necessary on a case-by-case basis, and may rely on credible security certifications such as HITrust/AOC which the vendor may provide as evidence of their security maturity.

PONDURANCE

PROCEDURE – RISK

- The NIST CSF assessment spreadsheet will be completed in which each column within the spreadsheet will reference the vendor being assessed. Once all of the documentation has been reviewed, the consultant will begin filling out the assessment with the information intake form provided by the vendor.

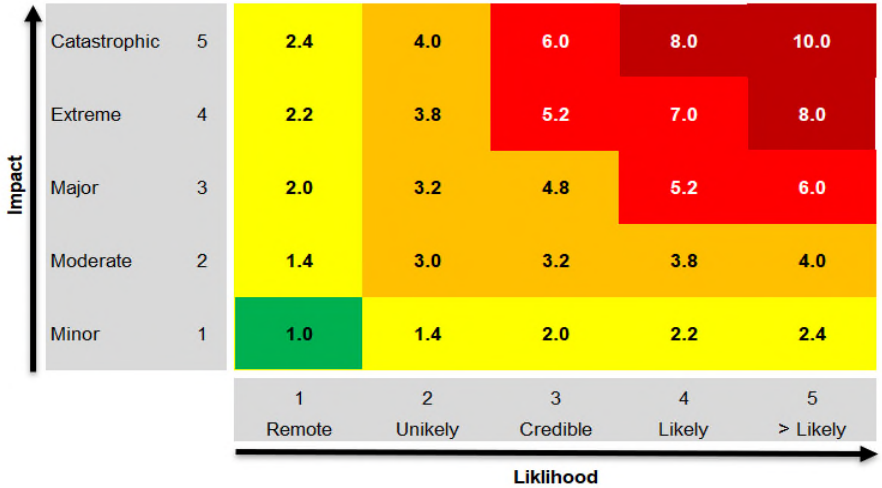
- For each question, the consultant will need to assess the following:
  - Business criticality of the system being assessed
  - Potential security risks and vulnerabilities of the application
  - Likelihood and impact of the potential security risks and vulnerabilities
  - Risk appetite of the organization
  - Previous security incidents of the organization.

PONDURANCE

THE RISK CALCULATION

Likelihood * Impact = Risk

(Control Status + Control Importance) (Business Criticality + Information Sensitivity)



PONDURANCE

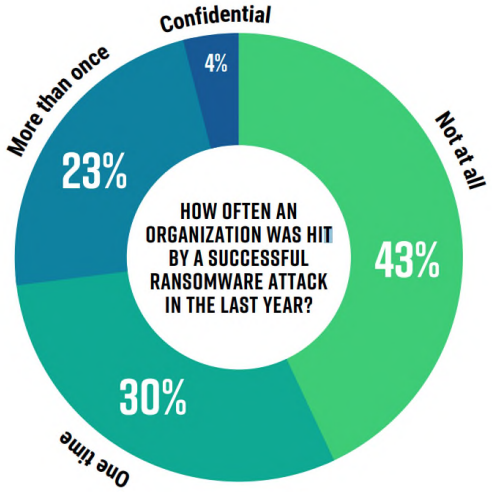
PROCEDURE - DETAILS

- Tried to build it for ease of use.
- We send intake form to vendor and it would be returned to us.
- We review vendor responses and any documentation provided including third party attestations (SOC report, AOC, HITrust).
- We document and score assessment.
- We provide recommendations and final assessment to client (remediation, reassessment cycle, etc.).
- Some providers already publish self assessments to the CSA Security, Trust & Assurance Registry (STAR) .
- Cyclic process – revisit assessments that have not been done in the last year

PONDURANCE

THIRD PARTY BREACHES

- With only a steady increase between 2019 and 2020, the number of third-party data breaches jumped 17% in 2021.
- What's behind the surge?
  - Ransomware accounts for 27% of the attacks



PONDURANCE

RECENT BREACHES

- March 2022
  - Microsoft Breached by Lapsus$ Hacker Group
  - Lapsus$ Group Breaches Authentication Company Okta
- August 2021
  - Databases and Account Details on Thousands of Microsoft Azure Customers Exposed

Source: https://firewalltimes.com/recent-data-breaches/

PONDURANCE

QUESTIONS

PONDURANCE