ISE® CENTRAL EXECUTIVE FORUM

Nominee Showcase Presentation

Parkland Hospital

3P-VRM Process

Shibu Thomas

CISO

Company Overview

Parkland

- Parkland Health & Hospital System is one of the largest public hospital systems in the country. The hospital averages about 51,000 admissions and 1 million outpatient visits annually.
- Premier services include a one of the best level I trauma centers in the nation, the second largest civilian burn center in the U.S. and a level III neonatal intensive care unit.
- The system also includes more than 30 community-based clinics and numerous outreach and education programs.
- In August 2015, Parkland opened its new $1.3 billion state-of-the art facility. The new Parkland Memorial Hospital added desperately needed space for better delivery of healthcare services to a growing population.
- Parkland named among Most Wired Hospitals for the past 4 years and won a 2017 HIMSS Enterprise Davies Award

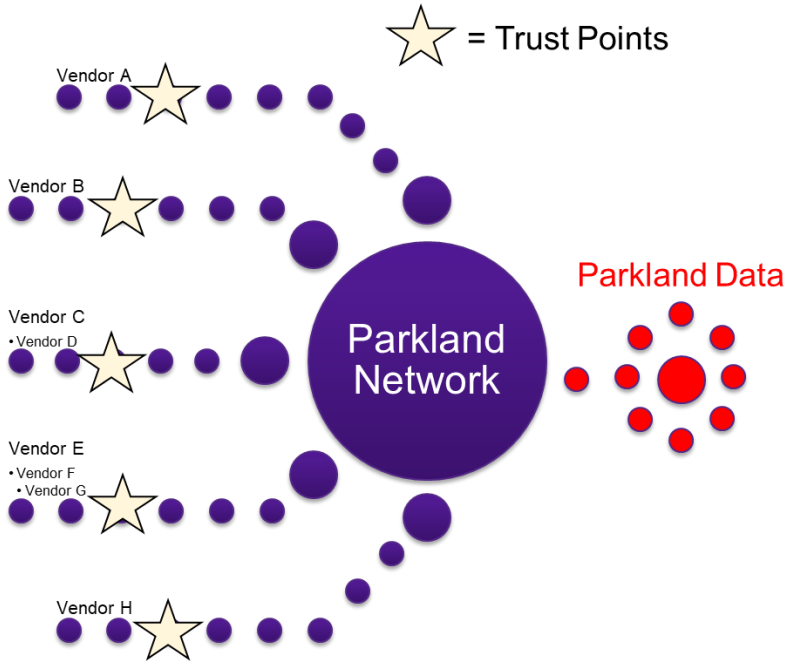
Why Vendor Risk Management?

- Parkland has classified vendor risk as having a high residual risk rating
- Parkland has services with approximately 250 IT vendors
- A Business Associates Agreement does not fully transfer risk
- Not just a healthcare problem - According to a Ponemon Survey, cybersecurity incidents relating to vendors are increasing and half of respondents said their organization experienced a data breach caused by a vendor

Project Goal

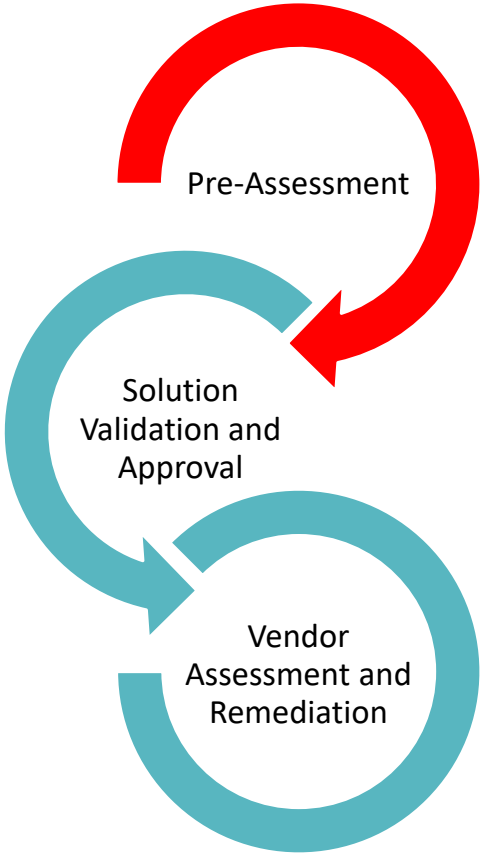
Develop a Vendor Risk Management Program

- Evaluate prospective vendors and IT solutions/services to ensure they meet standards (unvalidated pre-assessment)
- Implement internal process to validate IT solutions before contracts are signed
- Contract with a third party service to assist with full vendor assessments and remediation tracking



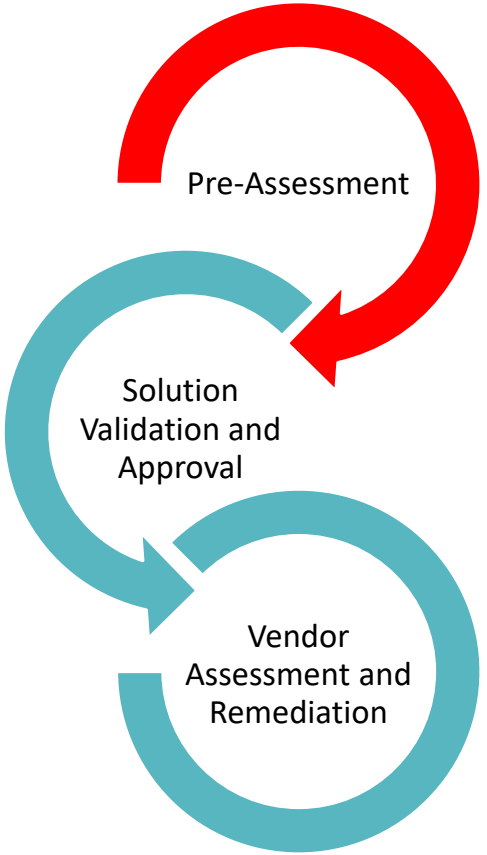
Phase 1: Pre-Assessment

- Parkland typically initiates a RFP for new IT solutions
- Prospective vendors must complete a questionnaire to determine if they meet Parkland standards
  - Includes both security and operating environment standards
- Vendors that don't meet minimum requirements are eliminated from contention



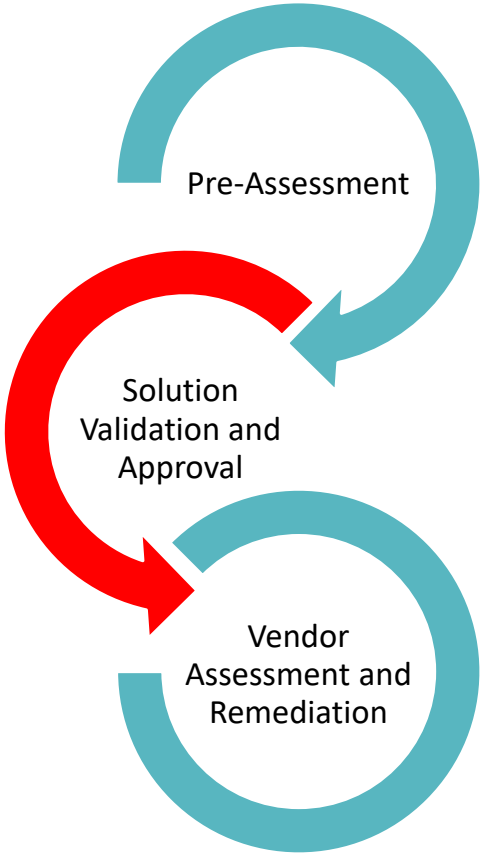
Phase 1: Keys to Success

- Leadership buy-in was a must. Organization had to be willing to give up control in purchasing IT solutions
- All IT purchases had to be funneled through a centralized process
- Supply-chain buy-in and training required to identify an “IT Purchase”
- Established “red lines”.
  - What are the deal killers?
  - What if “best of breed” solution didn’t meet requirements?
  - What if none of the solutions met requirements?
- Deep-dive at this phase is not practical



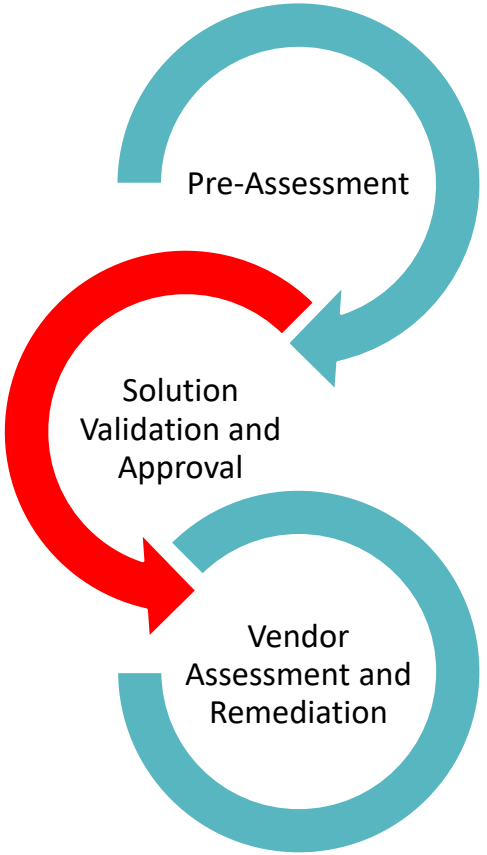
Phase 2: Solution Validation and Approval

- Utilize trust-but-verify approach by working with vendor to understand proposed architecture and reviewing documentation supplied by the vendor
  - Review may include reviewing data center details, ports/protocols application uses, details of encryption, etc.
- Additional certification documentation such as SOC II reports are taken into consideration
- Project will be provided an authorization letter with the status of approved, approved with contingencies or denied
- Contracts are signed when a vendor receives a status of approved or approved with contingencies



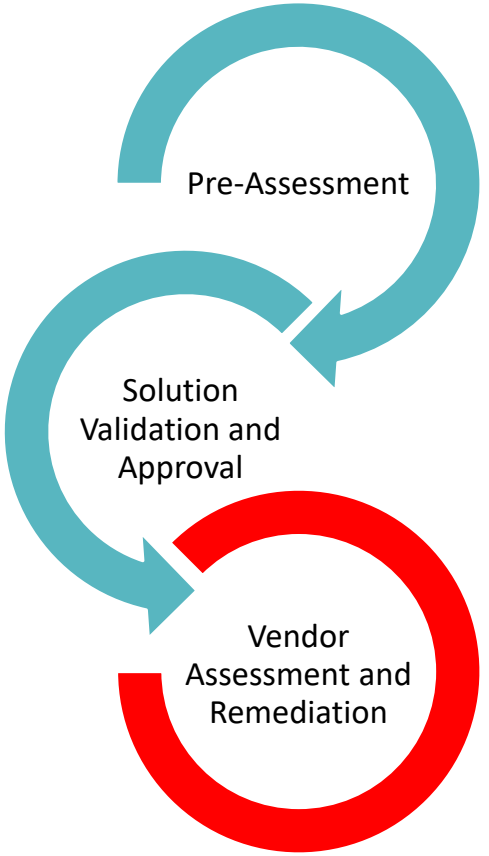
Phase 2: Keys to Success

- Educated IT application owner and project managers
- Process needed to be streamlined to prevent project drag
- Established “red lines”.
  - What are the deal killers?
  - Set expectations with business owners



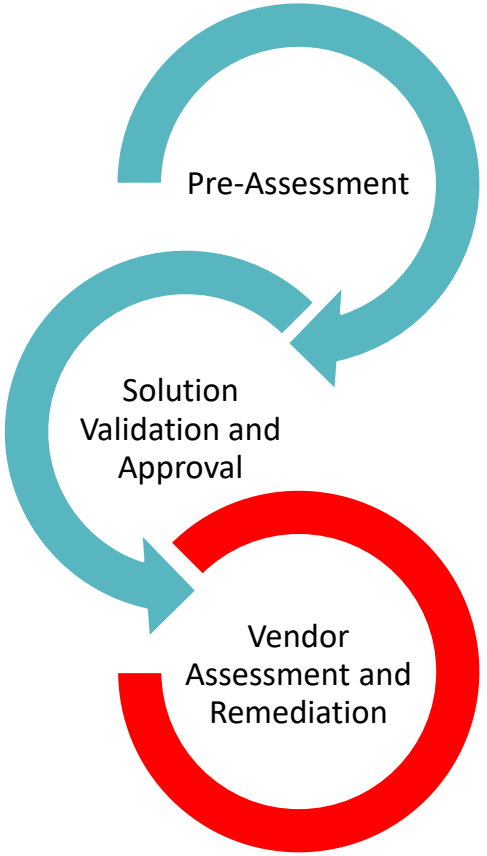
Phase 3: Vendor Assessment and Remediation

- Third party consultant conducts two-part review of vendor
  - Part 1 is a high level assessment based on publically available data
  - Part 2 is a full deep-dive that requires the vendor to respond to a detailed questionnaire
  - In lieu of questionnaire, vendor can provide a properly scoped SOC 2 Type 2 report or HITRUST certification
- Output is a vendor grade, detailed report and a recommended remediation plan
- Parkland works with vendor to come to an agreement on the remediation plan and third party consultant tracks remediation progress
- Vendors are continuously monitored for any significant changes to their risk posture



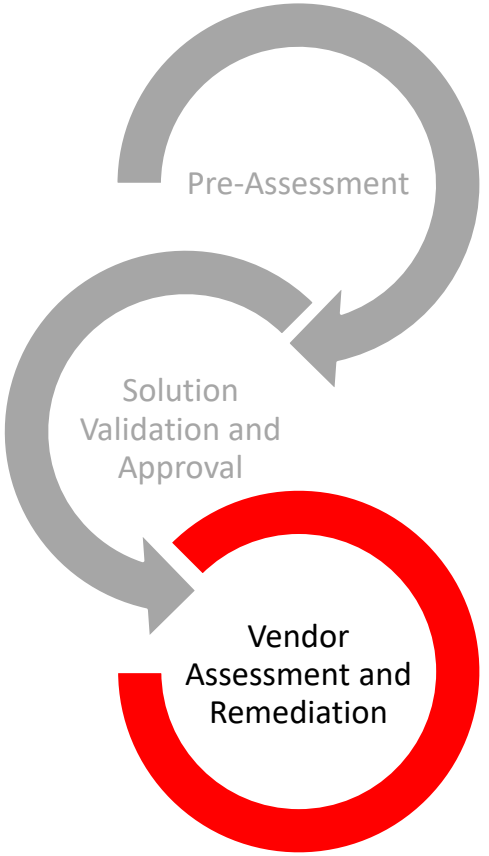
Phase 3: Keys to Success

- Included “right to assess” by third party in the contract with option of establishing NDA with vendor
- Parkland needed to remain engaged – not a “hands off” process
- Had to be willing to compromise on remediation plans and timelines
- Best results when process initiated early in the vendor relationship



What about existing vendors?

- Existing vendors are slowly being retrofitted through the Vendor Assessment and Remediation phase
- Results have been mixed with some vendors refusing to cooperate
  - Parkland response is based on potential impact based on the vendor's risk profile
  - Language will be updated at contract renewal or vendor will be eliminated through attrition



Project Results

1. Awareness of vendor risk management has improved significantly which federates this responsibility to the appropriate departments and teams in the organization
2. Since the full implementation in 2017, the exemption requests for security standards for new projects have declined by 23 percent, and continues to decline
3. Significant identified vendor risks have either been corrected or are in the process of being corrected

Lessons Learned/Best Practices

1. Organizational buy-in - develop a method to control purchases of IT solutions
2. Involve relevant departments, such as Contracts, Legal and Purchasing
3. Ensure the contract includes agreement to allow full assessment of the vendor
4. Establish “red lines”
5. Demand transparency from vendors to establish the new normal
6. It’s not always technology that has to be put in place to solve problems. People and processes alone can have a big impact in improving a company’s security posture

Thank you and Questions

Questions?

Contact Info: Shibu Thomas

- 214-590-4777
- shibu.thomas@phhs.org