Trust But Verify

An Argument For Security Testing Vendors

SANS Supply Chain Summit August 2019

Kyle Tobener

Director, Enterprise Security

@kylekyle

Rachel Black

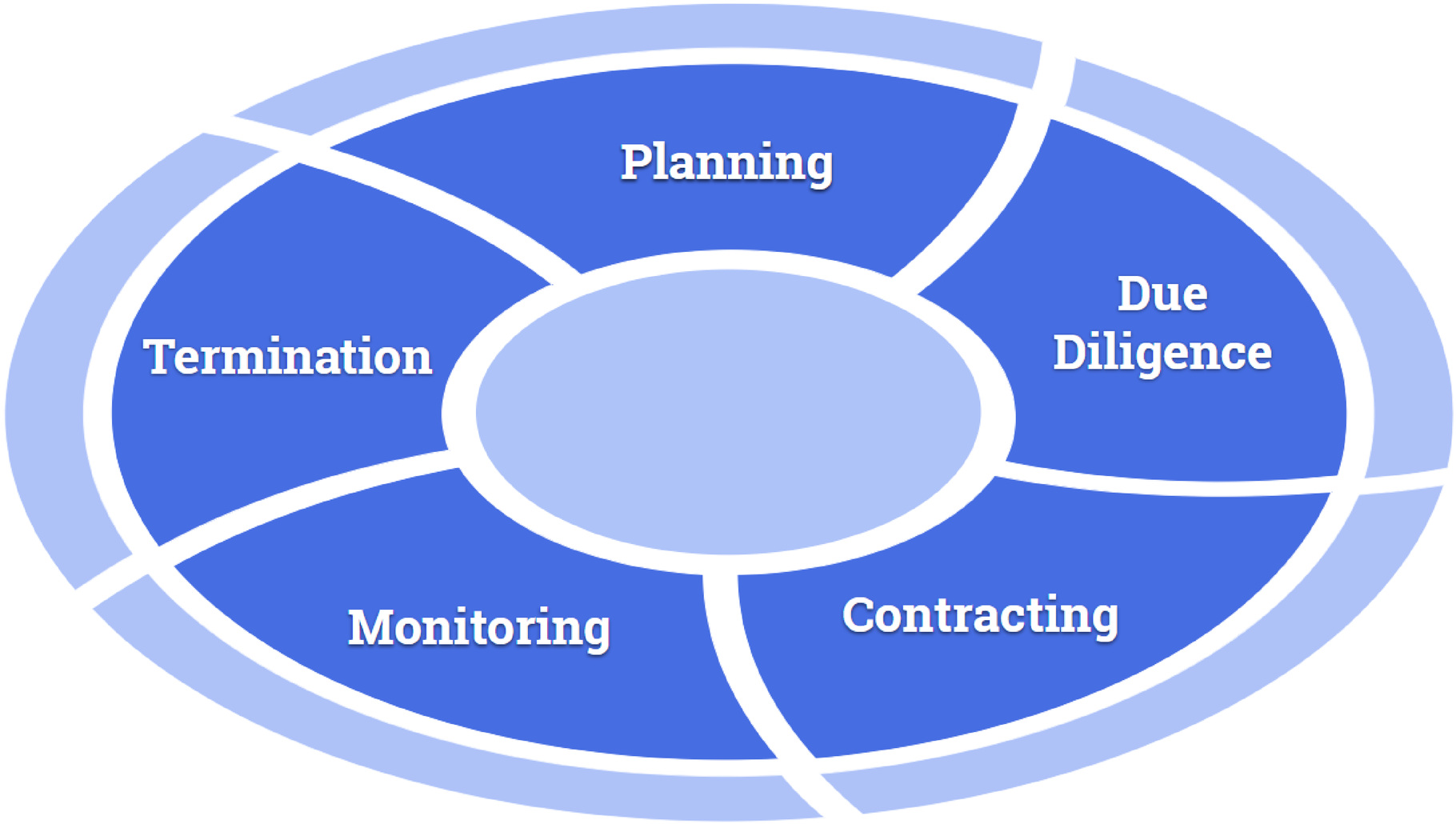
Sr. Manager, Application Security

Agenda

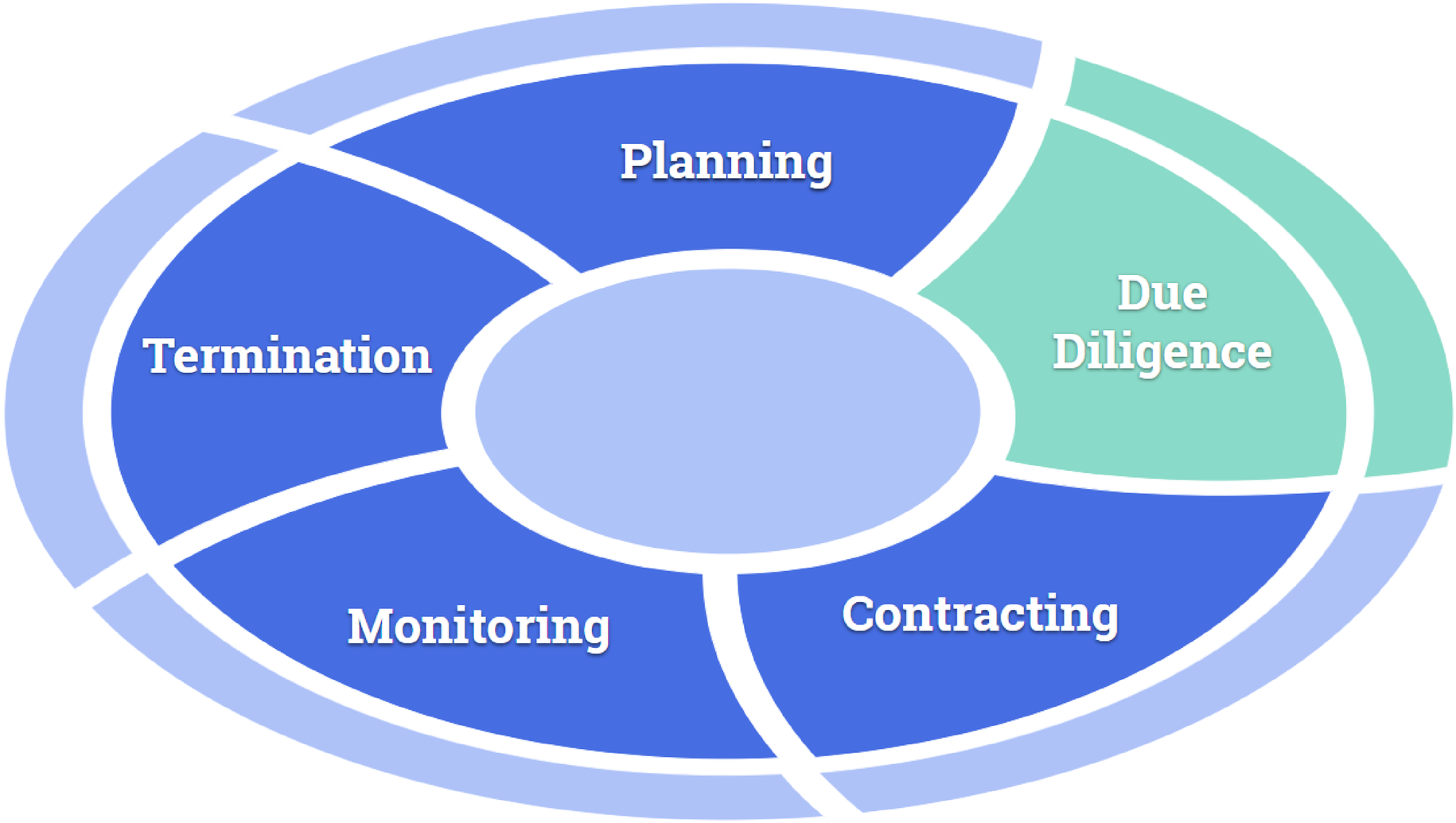
- Vendor Risk Management Basics
- Security Testing
  - Overall Process
  - Case Studies
  - Benefits
  - Challenges
- Wrap Up

Vendor Risk Management
Basics

Vendor Risk Management Lifecycle

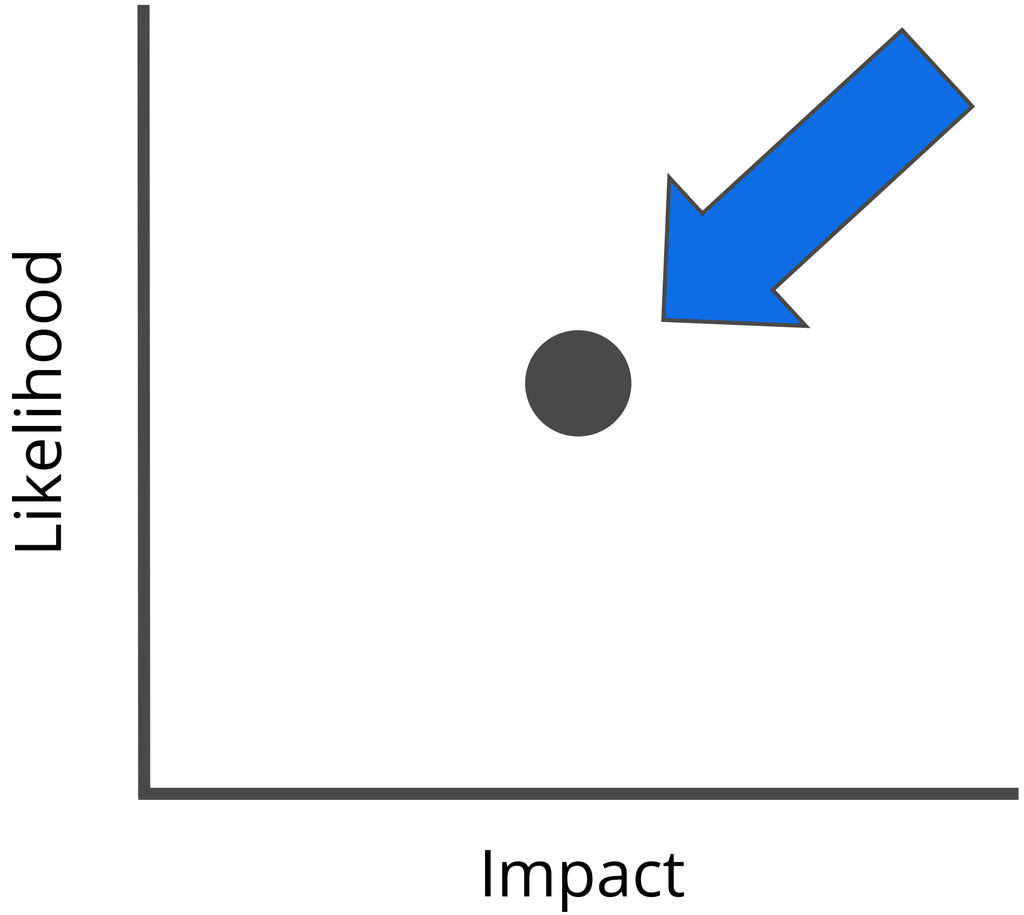


Vendor Risk Management Lifecycle



What is the Purpose?

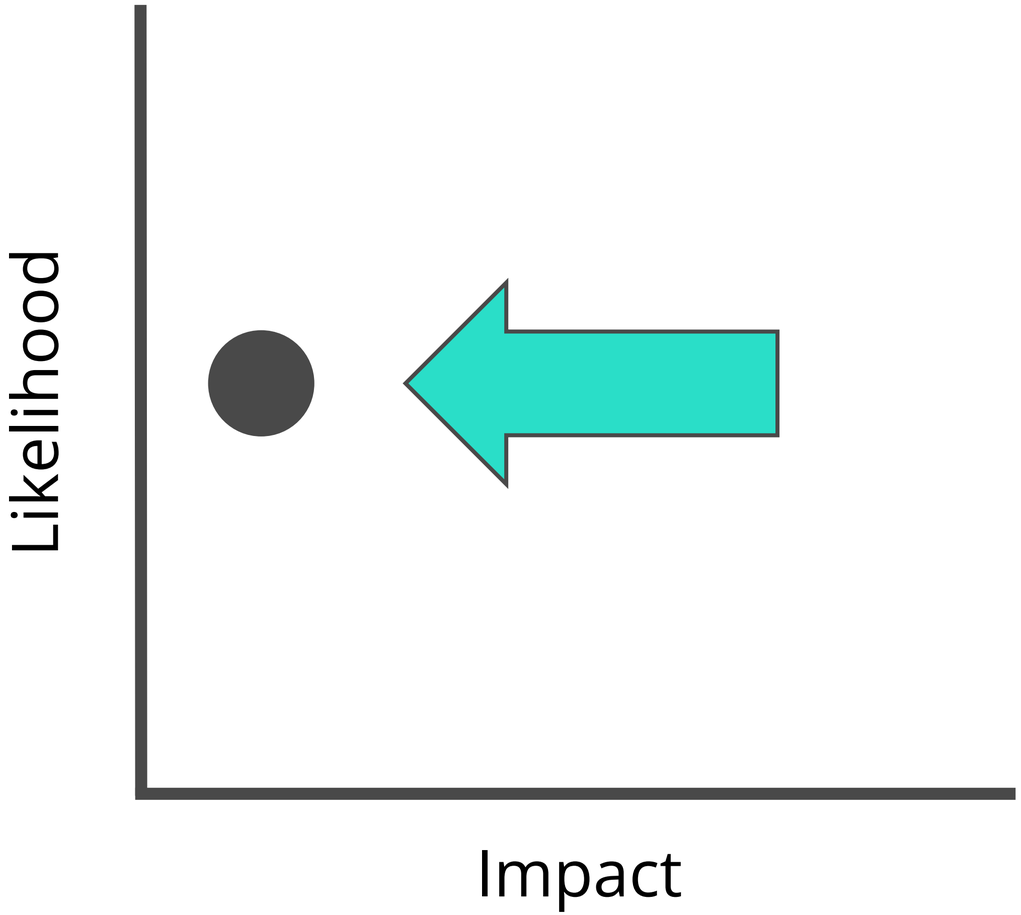
...to **reduce risk** to the Organization!



What is the Purpose?

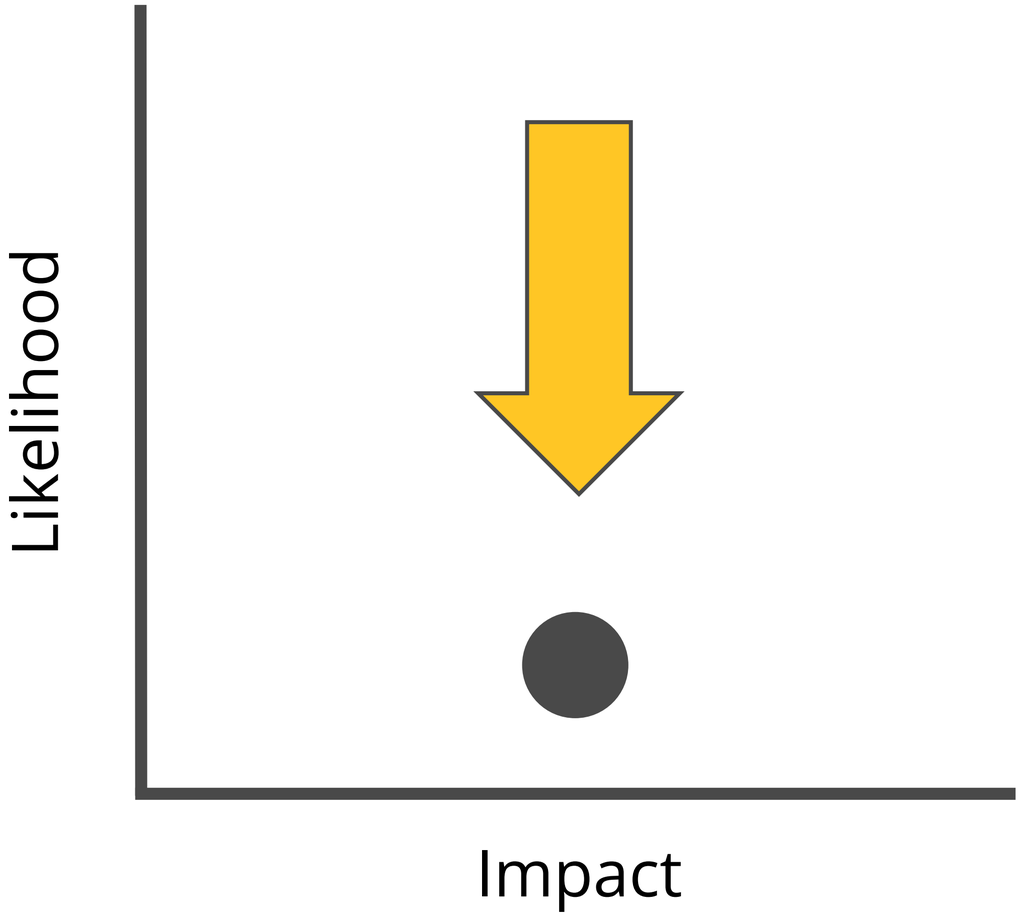
Reducing impact

is **easy**!



What is the Purpose?

Reducing impact is harder.



Approaches to Diligence

Questionnaire

Certifications

Security Testing

Questionnaire

Questionnaires **do not** evaluate breach likelihood effectively.

Vendor Security Alliance

SFG | SHARED ASSESSMENTS

Approaches to Diligence

~~Questionnaire~~

Certifications

Security Testing

Certifications

Compliance **does not**

equal Security

Approaches to Diligence

~~Questionnaire~~

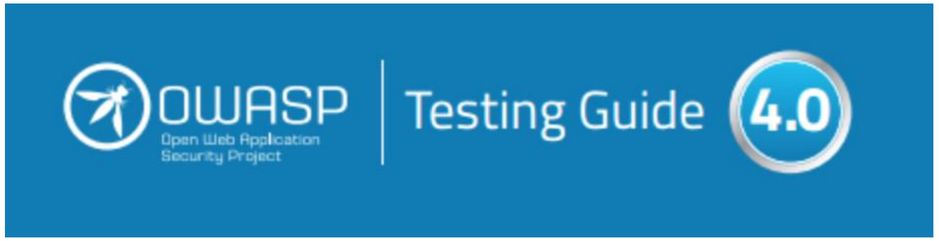
~~Certifications~~

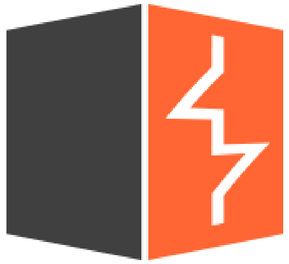
Security Testing

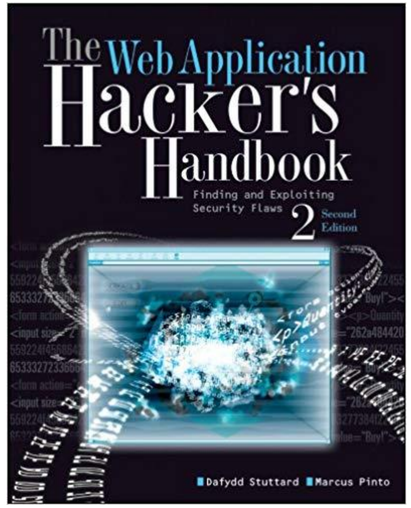
Security Testing
Overall Process

What defines “Security Testing”

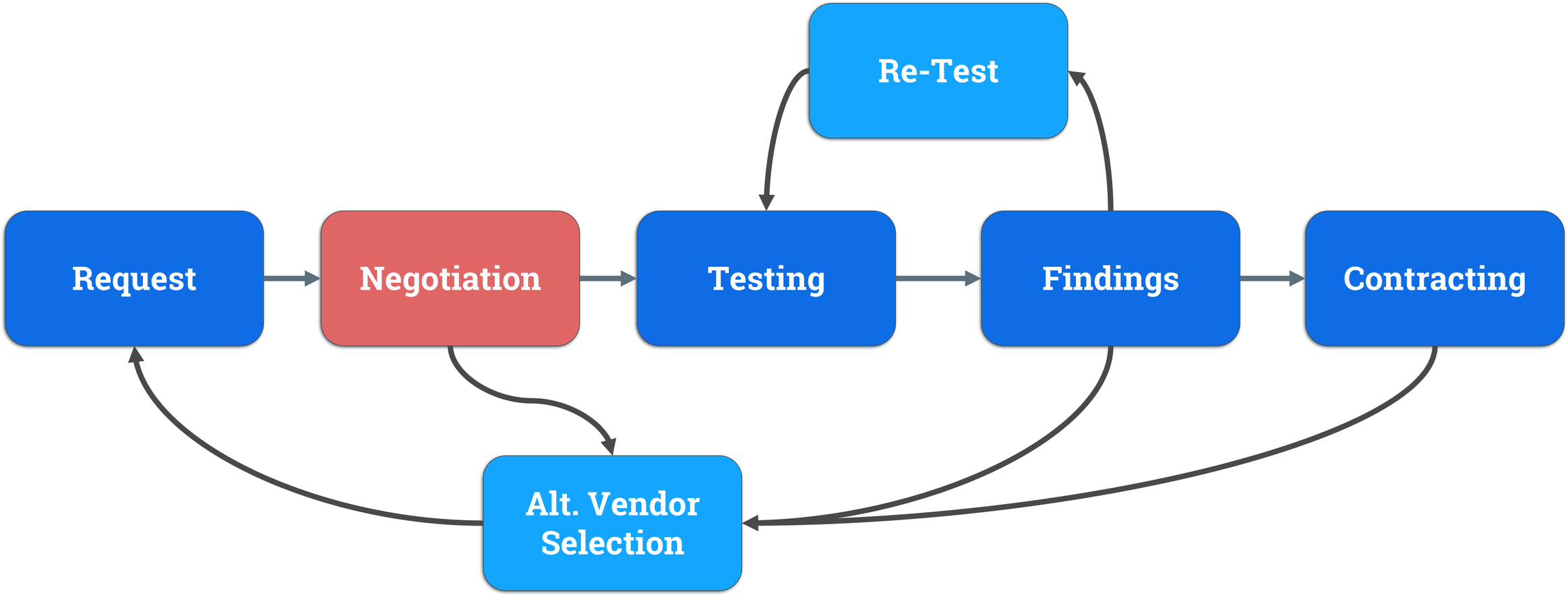
- Aka Penetration testing “light”
- Focus on data
- Find & report vulnerabilities
- Used to estimate breach likelihood







How does this actually work?



Why do all of this?

- **Increased** trust and transparency
- **Evaluate** technical maturity
- **Observe** responsiveness

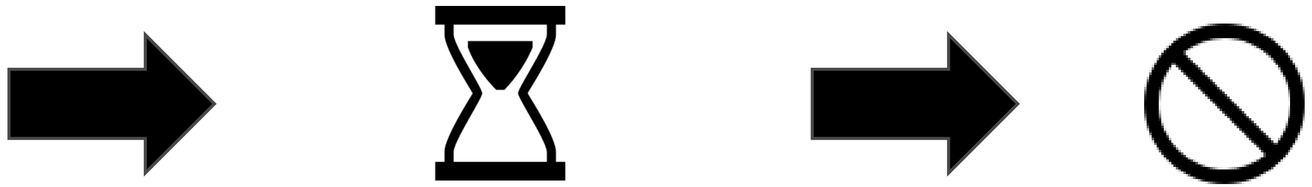
Security Testing
Case Studies

Case Study: Acme Healthcare

*"We're **HIPAA Compliant** so we're secure"*

*"**Most secure** solution on the market"*

*"Used by X, Y, Z and **THEY trust us**"*



4 Hours Into Testing

Case Study: Acme Benefits

*“We **have a process** for pentesting, just fill out this form”*

“Additional eyes are always great”

*“You should check out our **bug bounty** for ideas on where to look”*

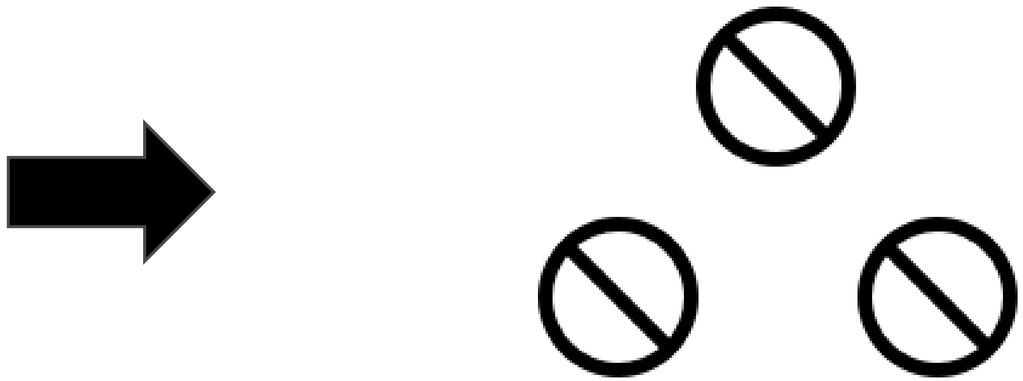
3 Days Into Testing

Case Study: Acme Software

*“We **don’t allow testing** of any kind”*

“Trust and transparency are not part of our culture”

*“Would you like a **letter from our CISO** attesting to our security posture?”*



Security Testing
Benefits/Challenges

Benefits

Company	Vendors	Everyone
• Better evaluation of security maturity • Evidence based influence	• “Free” Security Testing • Increased partnership	• More eyes leads to fewer bugs • Security influence on sales

Challenges

Company	Vendors	Everyone
• Scale Expensive • Talent hard to find • Point in time • Art, not science	• Potentially invasive • Legal hurdles	• Results under NDA • Difficult to share

Wrap Up

Thoughts for the Future

- Shared assessments frameworks should be expanded
- Existing vendors in the space don’t go far enough
- Increased transparency makes diligence overall easier

Key Takeaways

- Measuring likelihood in risk is very difficult
- Don’t rely completely on self-attestations
- Add security testing to your 3rd party risk management program

Thanks!

Any questions?