RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: PDAC-T06

Rethinking Efficient Third-Party Risk Management

Todd Inskeep
Director
Booz | Allen | Hamilton
@Todd_Inskeep

Do you have to have a third party risk management program?

So, what's driving 3rd party risk management programs?

- Contractual flow through
  - HIPAA security & privacy
  - GDPR & other privacy regulations (Australia, China, Russia, Brazil, California, & growing)
- Operational risk
- Liability management
- Regulatory requirements
  - Financial services (OCC, FFIEC, more?)

Third party programs can feel out of control

- Different requirements from different customers
- Competing approaches –
  - SSAE18
  - Shared assessments
  - Vendor-specific solutions
- Multiple security frameworks
- Lack of uniformity, even within industries
- Made-up questionnaires

Your 3rd party risk program is really two programs

Your infosec program

Demonstrating how you manage risk as a 3rd party to other companies

Your 3rd party program

Managing risk from your 3rd parties

Most companies are both **suppliers** and **consumers** of third party solutions

Are you a Third party? Or managing third parties?

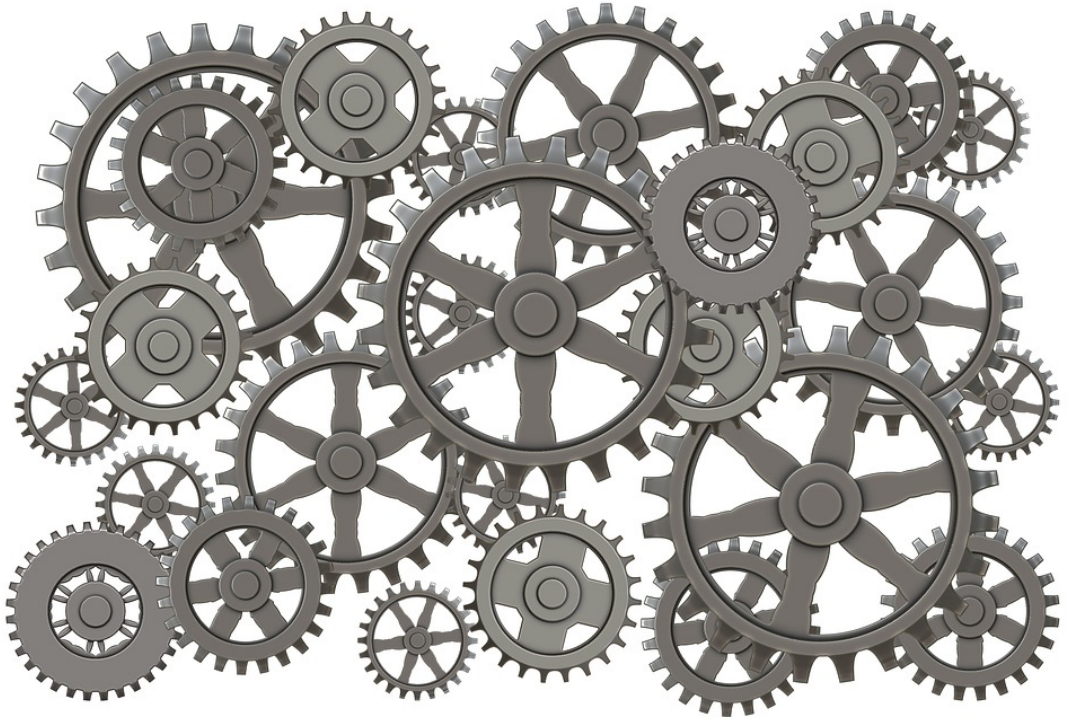
- You start off, the center of your universe…

- And pretty soon you can't find yourself

Before we go deep

Agenda

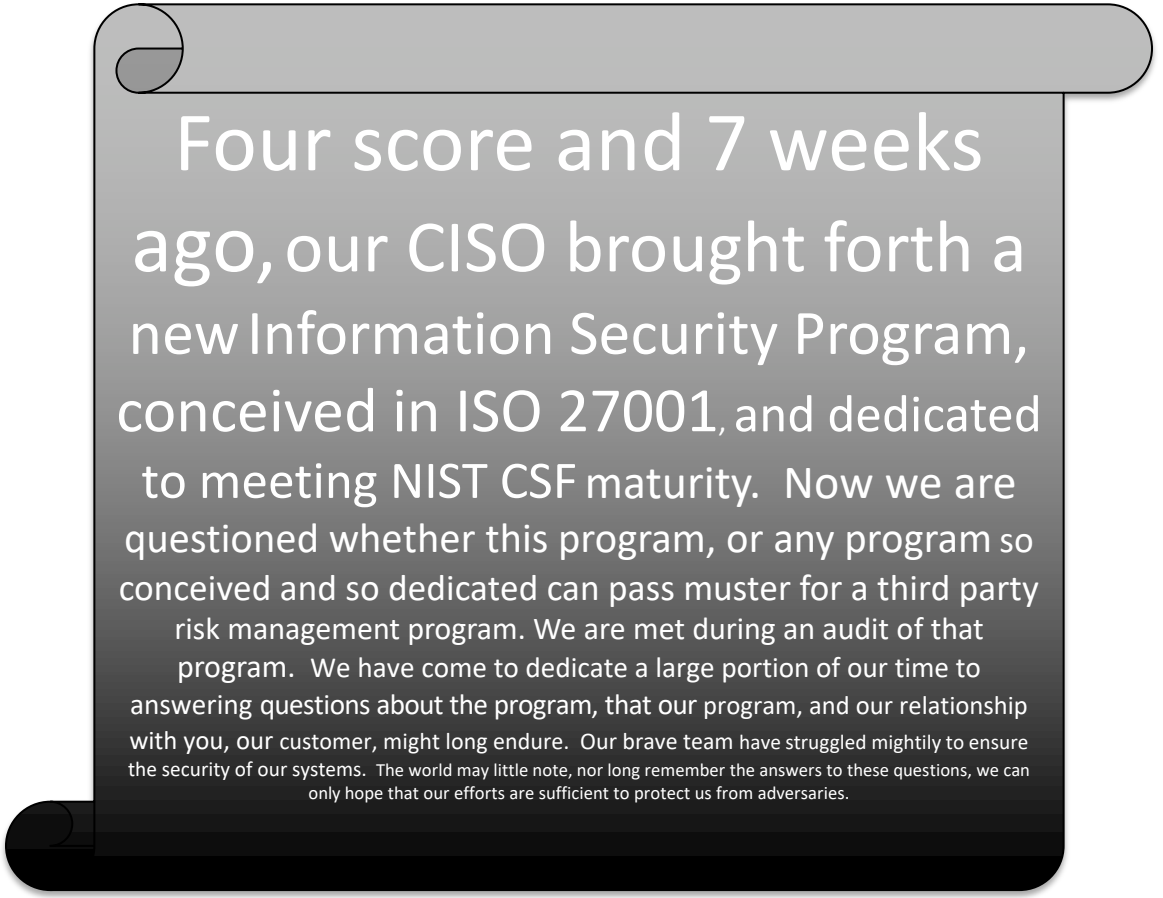
- Your information security program
- Your third party program
  - Why
    - Requirements
    - Risk Management
    - Comply
    - Operational Risk
    - Liability
  - How
  - What



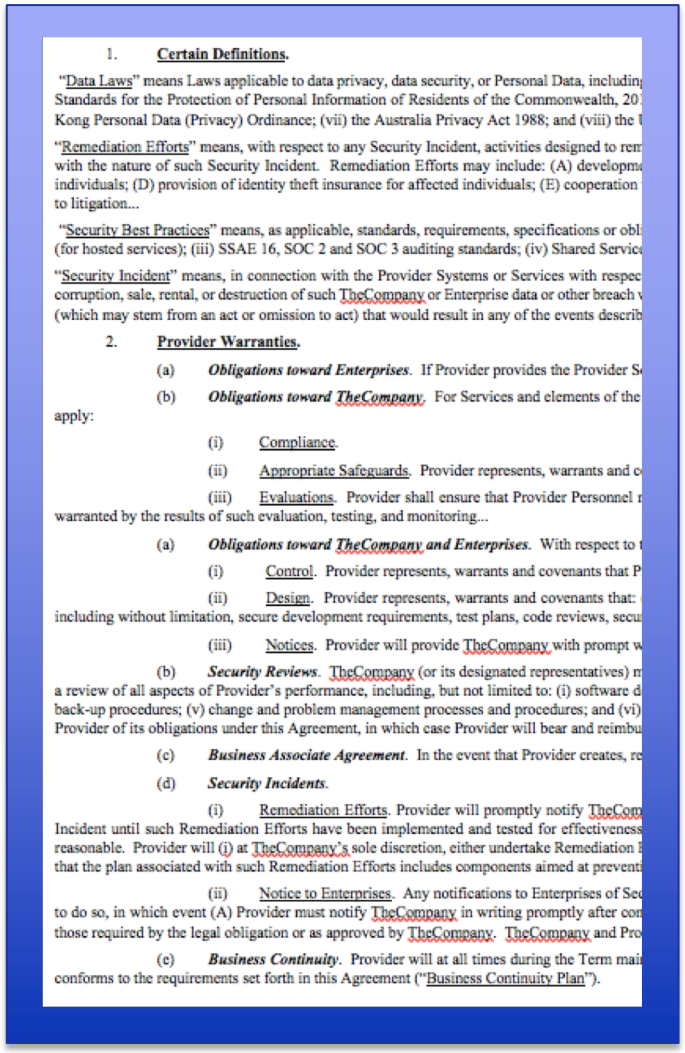
Note: Vendor mentions do not constitute an endorsement of any specific company or product .

Demonstrate your infosec program

- Build a ‘sharable’ document demonstrating your program’s compliance with and alignment to a framework
- Share the document instead of answering questionnaires
- Get external proof (especially if required) and re-use that proof as much as possible
  - SSAE 18
  - Shared assessments
  - CyberGRX
- Identify any specific contract requirements from customers
  - Ensure mechanisms to comply - for example breach notification requirements



Contract flow through and your infosec program



1. **Certain Definitions.**

"Data Laws" means Laws applicable to data privacy, data security, or Personal Data, including Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 Kong Personal Data (Privacy) Ordinance; (vii) the Australia Privacy Act 1988; and (viii) the U

"Remediation Efforts" means, with respect to any Security Incident, activities designed to rem with the nature of such Security Incident. Remediation Efforts may include: (A) developme individuals; (D) provision of identity theft insurance for affected individuals; (E) cooperation to litigation...

"Security Best Practices" means, as applicable, standards, requirements, specifications or obl (for hosted services); (iii) SSAE 16, SOC 2 and SOC 3 auditing standards; (iv) Shared Servic

"Security Incident" means, in connection with the Provider Systems or Services with respec corruption, sale, rental, or destruction of such TheCompany or Enterprise data or other breach (which may stem from an act or omission to act) that would result in any of the events describ

2. **Provider Warranties.**

(a) ***Obligations toward Enterprises.*** If Provider provides the Provider S

(b) ***Obligations toward TheCompany.*** For Services and elements of the apply:

(i) Compliance.

(ii) Appropriate Safeguards. Provider represents, warrants and c

(iii) Evaluations. Provider shall ensure that Provider Personnel warranted by the results of such evaluation, testing, and monitoring...

(a) ***Obligations toward TheCompany and Enterprises.*** With respect to

(i) Control. Provider represents, warrants and covenants that P

(ii) Design. Provider represents, warrants and covenants that: including without limitation, secure development requirements, test plans, code reviews, secu

(iii) Notices. Provider will provide TheCompany with prompt w

(b) ***Security Reviews.*** TheCompany (or its designated representatives) a review of all aspects of Provider's performance, including, but not limited to: (i) software d back-up procedures; (v) change and problem management processes and procedures; and (vi) Provider of its obligations under this Agreement, in which case Provider will bear and reimbu

(c) ***Business Associate Agreement.*** In the event that Provider creates, re

(d) ***Security Incidents.***

(i) Remediation Efforts. Provider will promptly notify TheCom Incident until such Remediation Efforts have been implemented and tested for effectiveness reasonable. Provider will (j) at TheCompany's sole discretion, either undertake Remediation that the plan associated with such Remediation Efforts includes components aimed at preventi

(ii) Notice to Enterprises. Any notifications to Enterprises of Sec to do so, in which event (A) Provider must notify TheCompany in writing promptly after con those required by the legal obligation or as approved by TheCompany. TheCompany and Pro

(e) ***Business Continuity.*** Provider will at all times during the Term mai conforms to the requirements set forth in this Agreement ("Business Continuity Plan").

- Virtually every new contract includes security requirements
- With provisions for verification by:
  - Questionnaires,
  - Interviews,
  - And potentially audits
- Note specific provisions – for contract compliance, and to protect your organization
- <u>Often copied and pasted without regard to your specific products or services</u>

Identifying contract requirements

Capturing requirements

- Contract requirements come in many forms
  - Addendums & references
  - Jurisdictional regulations (california, china, russia, EU, etc)
- Use spreadsheets and GRC tools to capture these specific requirements
- Track changes in requirements

Ensuring compliance

- Establish mechanisms to ensure compliance
- Automate compliance where possible
- Use reporting and metrics to support compliance
- Breach notification is quickly becoming a key area
- Other concerns will be strengthened over time

Remember, compliant is not secure – but compliance is contractually required

Engage your customers

- Work with your business teams to identify your most important customers
- Meet with the CISO/security team and understand how your security impacts your customer's security and risk
- Understand how your customers view your security
- Determine where real program changes are warranted
- Explore conducting joint incident response exercises
- Participate in customer advisory board activities with the business

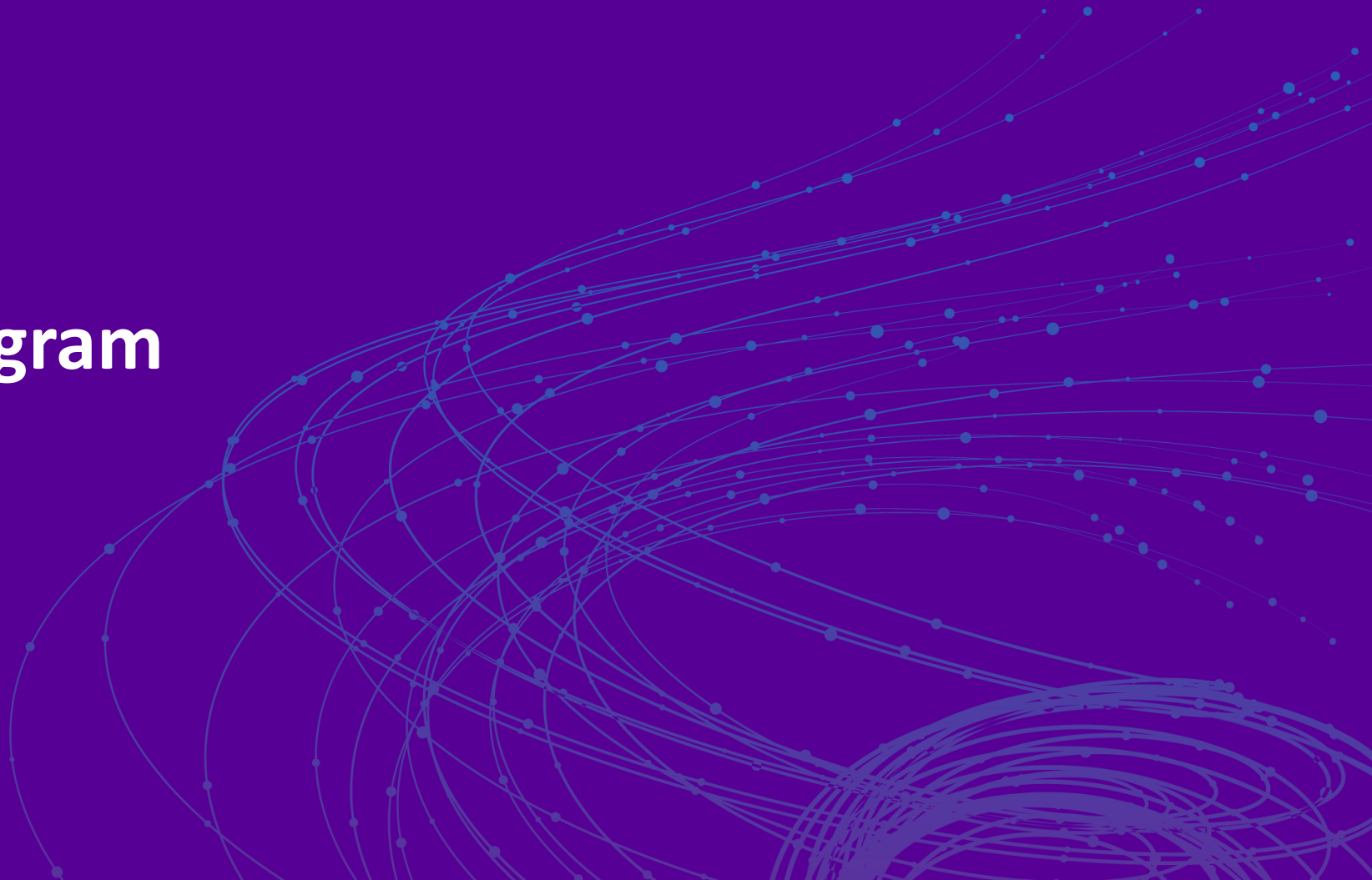
Get to know your customers before an incident forces you to become friends

Last thoughts on your information security program

- Backstop your program with appropriate insurance: business, cyber, operations, self-
- Representing your program can be costly – negotiate with your business partners about resources
- Customers shouldn't expect to have *new* security requirements met for free
- Finally, external risk scorecards can be misleading, investigate and challenge them appropriately
  - These scorecards should be treated like tools, *not* tablets from the mountaintop

RSAConference2019

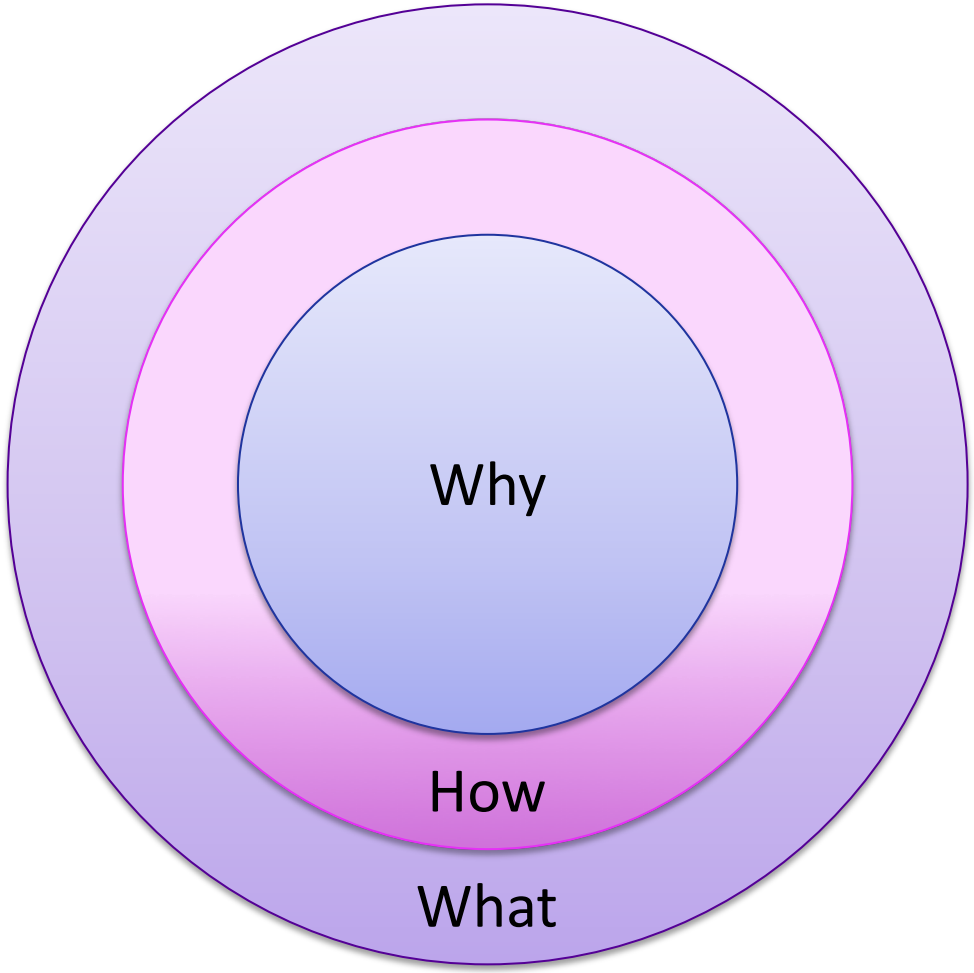
3rd Party Program



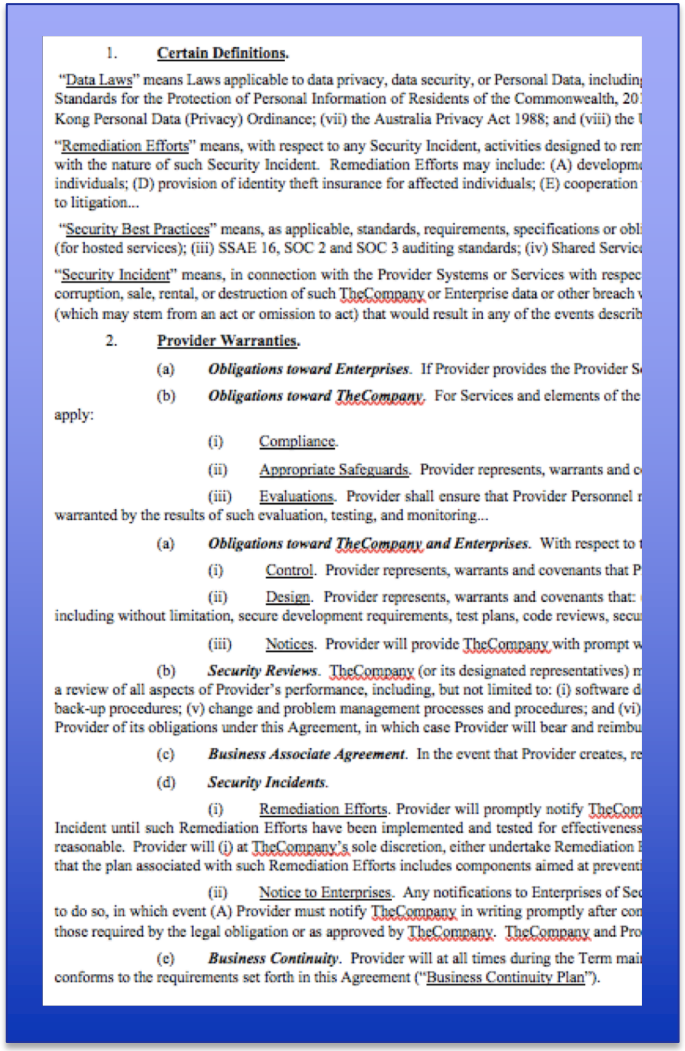
Forge your 3rd party program carefully

Start with why - why do you have a program?

- To pass **customer requirements** and expectations on to your vendors?
- To **manage risk** from your vendor's?
- To **comply** with external requirements?
- To **manage operational risk**?
- To **manage liability**?



Your requirements for 3rd parties



1. **Certain Definitions.**

"Data Laws" means Laws applicable to data privacy, data security, or Personal Data, includin
Standards for the Protection of Personal Information of Residents of the Commonwealth, 20
Kong Personal Data (Privacy) Ordinance; (vii) the Australia Privacy Act 1988; and (viii) the

"Remediation Efforts" means, with respect to any Security Incident, activities designed to rem
with the nature of such Security Incident. Remediation Efforts may include: (A) developm
individuals; (D) provision of identity theft insurance for affected individuals; (E) cooperation
to litigation...

"Security Best Practices" means, as applicable, standards, requirements, specifications or obl
(for hosted services); (iii) SSAE 16, SOC 2 and SOC 3 auditing standards; (iv) Shared Servic

"Security Incident" means, in connection with the Provider Systems or Services with respec
corruption, sale, rental, or destruction of such TheCompany or Enterprise data or other breach
(which may stem from an act or omission to act) that would result in any of the events describ

2. **Provider Warranties.**

(a) ***Obligations toward Enterprises.*** If Provider provides the Provider S

(b) ***Obligations toward TheCompany.*** For Services and elements of the
apply:

(i) Compliance.

(ii) Appropriate Safeguards. Provider represents, warrants and c

(iii) Evaluations. Provider shall ensure that Provider Personnel
warranted by the results of such evaluation, testing, and monitoring...

(a) ***Obligations toward TheCompany and Enterprises.*** With respect to

(i) Control. Provider represents, warrants and covenants that P

(ii) Design. Provider represents, warrants and covenants that:
including without limitation, secure development requirements, test plans, code reviews, secu

(iii) Notices. Provider will provide TheCompany with prompt w

(b) ***Security Reviews.*** TheCompany (or its designated representatives)
a review of all aspects of Provider's performance, including, but not limited to: (i) software d
back-up procedures; (v) change and problem management processes and procedures; and (vi)
Provider of its obligations under this Agreement, in which case Provider will bear and reimbu

(c) ***Business Associate Agreement.*** In the event that Provider creates, re

(d) ***Security Incidents.***

(i) Remediation Efforts. Provider will promptly notify TheCom
Incident until such Remediation Efforts have been implemented and tested for effectiveness
reasonable. Provider will (j) at TheCompany's sole discretion, either undertake Remediation
that the plan associated with such Remediation Efforts includes components aimed at preventi

(ii) Notice to Enterprises. Any notifications to Enterprises of Sec
to do so, in which event (A) Provider must notify TheCompany in writing promptly after cor
those required by the legal obligation or as approved by TheCompany. TheCompany and Pro

(e) ***Business Continuity.*** Provider will at all times during the Term mai
conforms to the requirements set forth in this Agreement ("Business Continuity Plan").

- What requirements are you placing on your vendors?
- Are they realistic and balanced?
- Can they be verified?
- How much will you spend on verification?
- What proof is enough?

- Can you leverage what others are doing?

Manage risk from vendors

Kinds of 3rd party risk

Reputational Risk

Compliance with
Security Standards

Secure Design

Contractual Liability

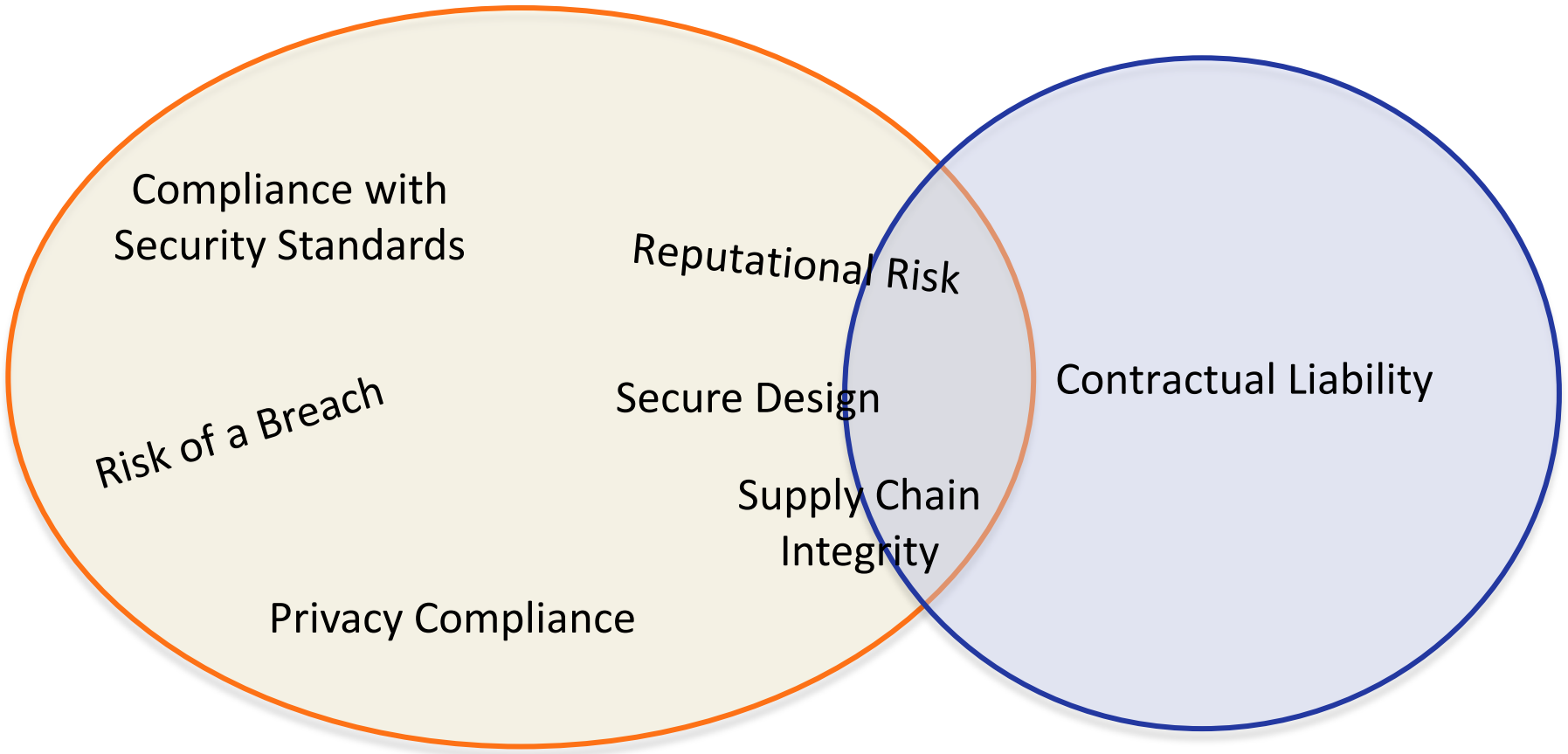
Risk of a Breach

Supply Chain
Integrity

Privacy Compliance

Manage risk from vendors

Kinds of 3rd party risk

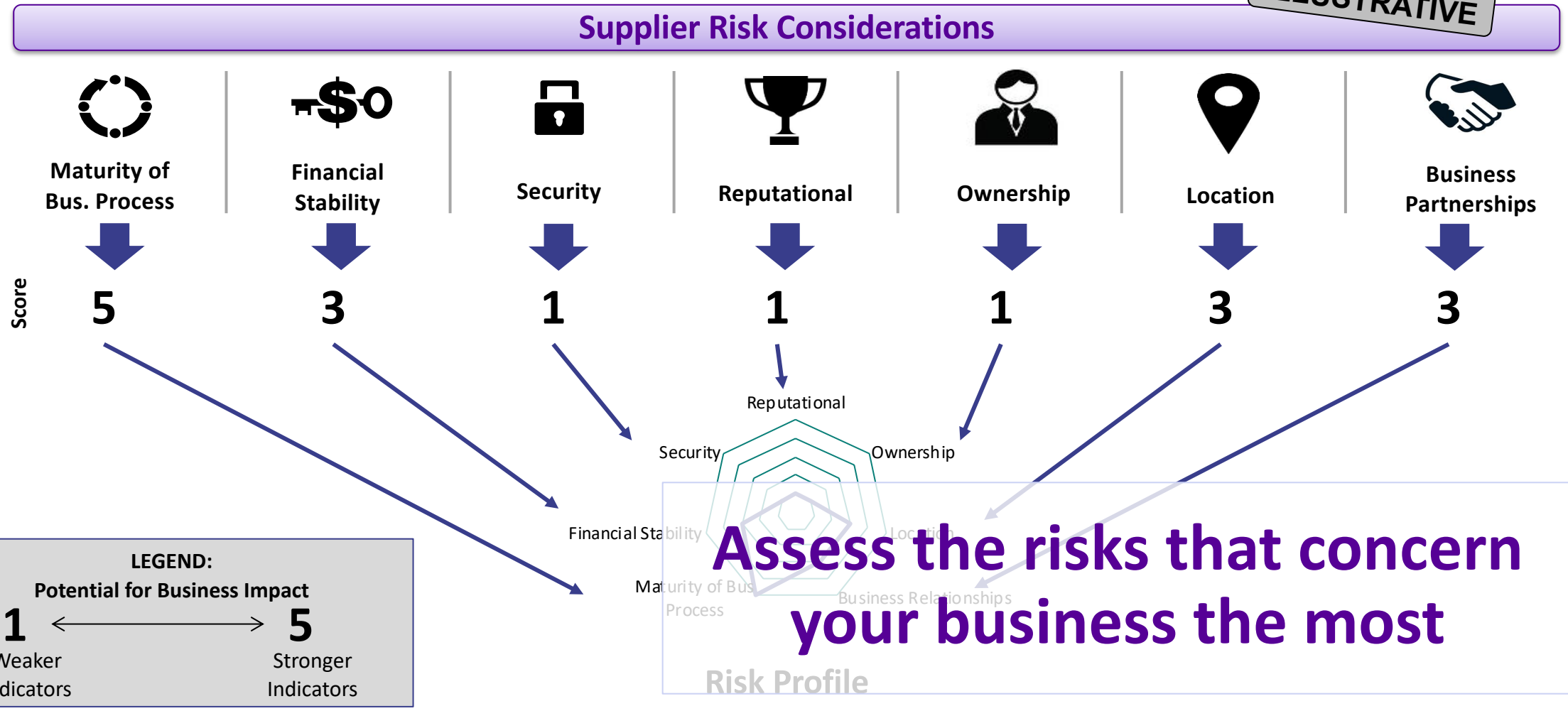


- 3rd party risks we can control
- 3rd party risks we can't control

Risk Mngmt

You can assess many kinds of risk from third parties

ILLUSTRATIVE



Assess the risks that concern your business the most

Complying with external requirements

Financial services

- Regulators expect banks to perform due diligence and ongoing monitoring for all 3rd-party relationships.
- Due diligence should be specific to, each third-party relationship.
  - Consistent with the level of risk and complexity posed by each third-party relationship.
  - For critical activities, monitoring will be robust, comprehensive, and appropriately documented.
- For low risk activities, this should follow the bank's established policies and procedures for due diligence and ongoing monitoring.

HIPAA & Health

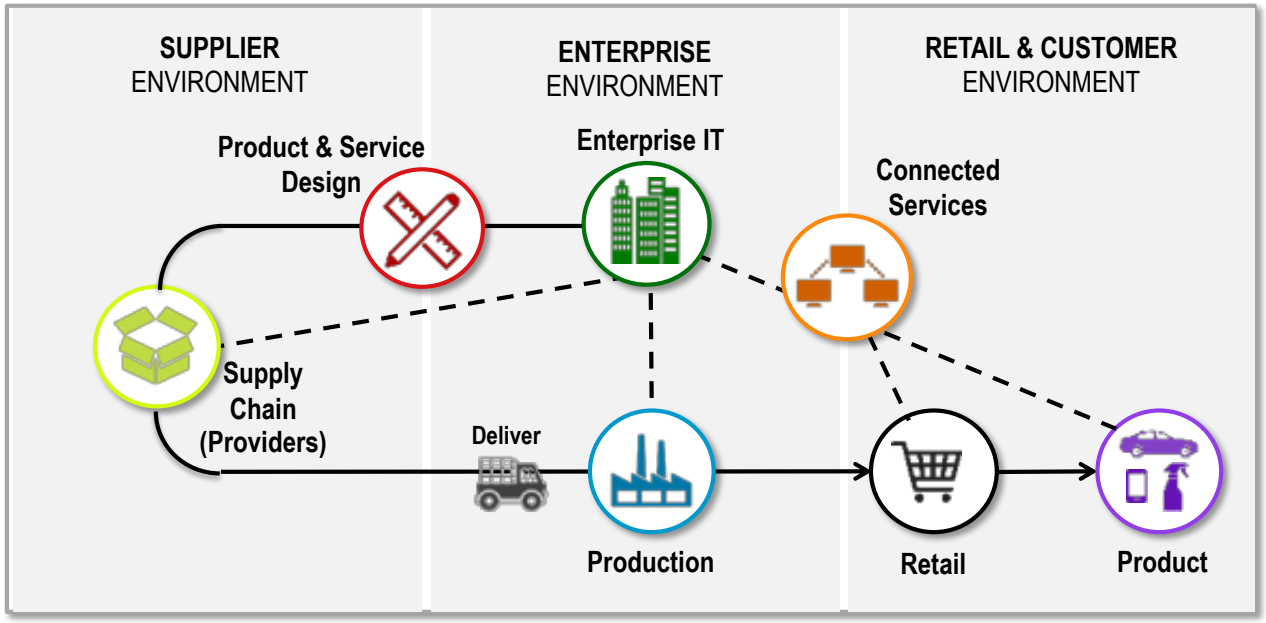
- Any third party that contacts PHI through the work it performs is a business associate, or BA.
- Both parties must have a contract detailing commitments to compliance
  - Providing assurances relating to the safeguarding of phi or the electronic equivalent, ephi
  - Before granting any level of access to PHI/ ephi

Privacy & GDPR

- GDPR deepens or adds requirements :
  - Article 28, requires contractual protections with data processors and their sub-processors.
  - Article 30, "requires data processors to maintain an inventory of the eu personal data they host;
  - Article 32, requires data processors (and subs) to implement information security controls to protect data;
  - Article 33, requires speedy breach notification
  - Article 36, requires data processors to provide impact assessments (dpias) to their clients.
- Bottom line: contractually establish SLAs

Operational

Manage operational risk



- Tied to critical business operations and the ”crown jewels” of that business or businesses
- Unique to each organization; may need to be refreshed and updated as your organization changes
- Requires the security team to deeply understand the business
- Requires business engagement to find nuances of specific business operations
- Follow the money, especially revenue
- Develop enterprise risk management processes, frameworks, metrics and reporting
- Evaluate all third parties and triage based on multiple factors.

Side Note: Companies should be especially deliberate in choosing security vendors;
Balance streamlining operations and cost efficiency with managing the associated risks of outsourcing.

Liability

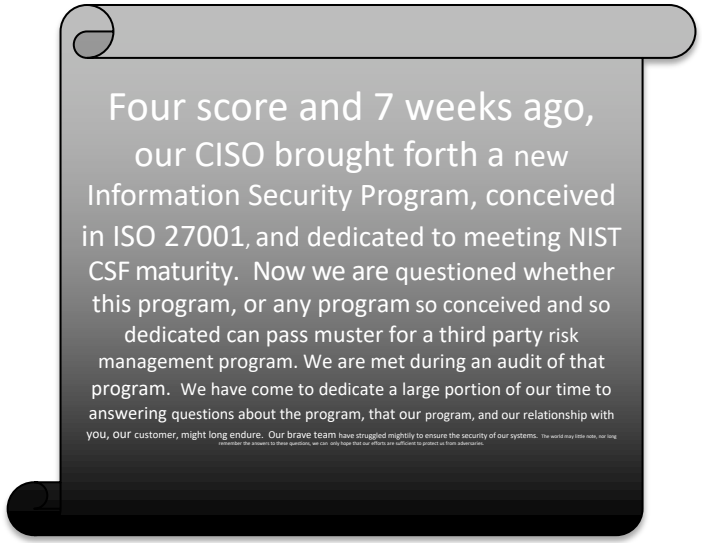
Managing liability

- Establish standard language in contracts, with specific, relevant requirements
(ie not 27001 compliance for every contract & purchase)
  - Identify specific requirements, especially critical service levels (for example breach notification)
  - Use a consistent framework where you have control
- Contractual indemnity clauses can only cover some risk transfer
- Track compliance by 3rd parties – if you require an SSAE-18, did you get one?
Could be low level, checklist, well maintained, by anyone
- Collect 3rd party proof only when needed, but reuse/accept 3rd party proof
  - Use a standard checklist – don't build your own

Liability

Minimize most requests to suppliers

- Require minimum compliance in contracts
- Presume vendors are compliant with the contract – rely on contract law
- Track compliance for a formal program, limit verification
- Leverage the fact that other companies are verifying and auditing vendor compliance.
- Verify only the most critical suppliers (who are unlikely to be verified by someone else)

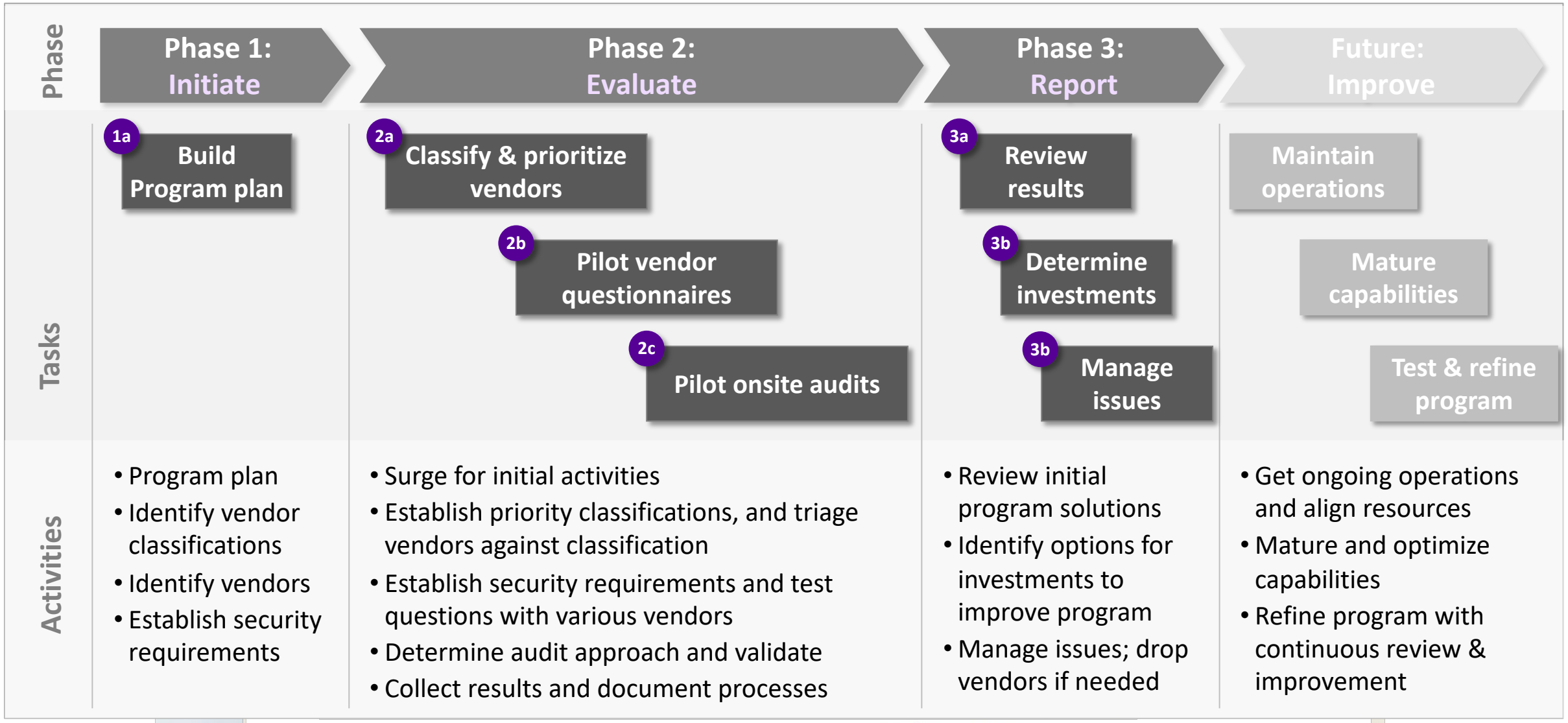


Ask for their proof:

- **SSAE 18**
- **Shared Assessments**
- **CyberGRX**
- **Other?**

HOW

Standard approach to building a program



Third party risk management is an ongoing process

- Starts with a project to design, build, and establish operations
- Then it has to operate over time
- With refinements as you learn and requirements change

Some best practices worth highlighting

- A documented end-to-end 3rd party risk management process with identified stakeholders and sub-processes that covers "all" aspects of supplier risk including financial due-diligence, legal assessments, personnel screening, contract compliance verification, and risk scoring.
- The process includes business owners, technology associates, security experts, risk management personnel, and legal, contracts, and other departments as appropriate.
- Technology automates the 3rd party risk management process and manages the prioritization of vendors and compliance checks; specifically, databases and automation to ensure regular reviews are conducted, metadata to capture business and technology points of contact, etc.
- Trained and certified (preferably dedicated) resources are hired and retained to manage 3rd party security. CISSP or similarly certified security experts combined with internal training on company risk processes, source selection, and contracting facilitates highly effective 3rd party risk management.
- Critical 3rd party solutions are reviewed from an attacker perspective with both automated and manual testing to limit vulnerabilities, proactively prevent foreseeable threats, and eliminate known challenges (like cross-site scripting) prior to deployment.

HOW

Engage your most important suppliers

- Identify your key suppliers; prioritized by risk and value to your business
- Plan and hold a vendor security day conference;
  - Use it to emphasize the importance of security to your business
  - Make securing your business personal for the suppliers
- Meet the CISO at important suppliers
- Use automated tools as canaries for major changes in critical suppliers
- Vendor day ”conference”
  - Emphasize importance of security to business
  - Make it about business and be personal
  - Ask for help – share security challenges

Vendor Day Example

- Agenda
  - Welcome Breakfast
  - Code of Conduct
  - Introduction to IT Leadership Team
  - Corporate Business & Information Technology’s Response
    - Commercial Business Challenges
    - Research & Development
    - Manufacturing and Supply Chain
    - General &Administrative
  - IT Portfolio & Project Management
  - Information Security
  - Workshops
  - Closing Remarks/Q&A
- Goals
  - Demonstrate shared values
  - Identify additional business opportunities
  - Develop partnerships
  - Know your couterparts

So, What?
What do you spend effort on to be efficient??

Spend energy where you can impact results

Why	Effort: Minimal	Optimal	Maximal
Customer requirements	✓		
Vendor risk		✓	
Compliance	✓		
Liability		✓	
Operational risk		✓	
Contract Compliance			✓

Optimizing can help address common industry challenges

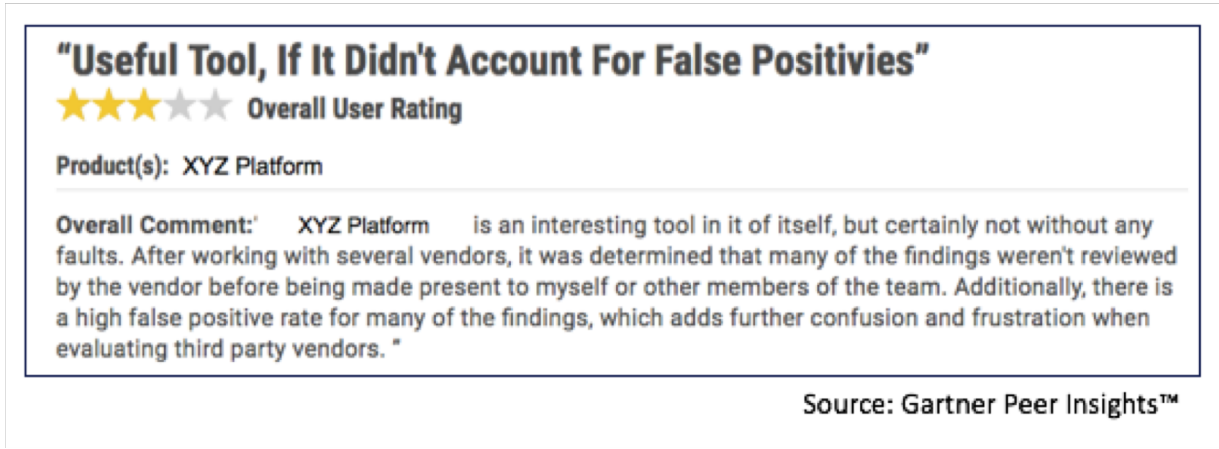
- Prioritizing 3rd party risk and security management against competing security program portfolio activities and priorities
- Automation tools for 3rd party security (and risk) management are not comprehensive; for example, just tracking points-of-contact and related metadata due to personnel changes can be a full-time job.
- Many contract and regulatory requirements focus on vulnerabilities and compliance making it hard to prioritize vendors based on risk or threat modeling.
- Hiring, developing, and retaining employees with the proper expertise and skill-set is challenging; specifically training and certifying individuals to conduct vendor security assessments and adopting a risk management culture.
- Enforcing sub-vendors' information security practices around data storage, processing, and transmission requires a real focus on understanding actual operating practices.

Remember to look for some partners

- Auditors & SSAE-18
- SharedAssessments
- CyberGRX

- External scanning & reporting companies
  - Security Scorecard
  - BitSight
  - Risk Recon
  - Others…

- Push your industry ISAC to drive common approaches:
  - Similar 3rd parties, similar needs
  - Reduce system noise and turbulence
  - Highlight opportunities to work together
  - Drive the right behaviors



Apply these lessons at home

- Review both aspects of your program (up and down)
- Look beyond the ”traditional” for your 3rd party risk program
- Remember the things you can and can’t change at 3rd parties
- Right-size your activities for your business operations and your specific 3rd parties
- Review your resource and planning needs
- Adjust your strategy
- Focus your program execution on the things you can control

QUESTIONS

RSAConference2019

Thank You

FOR MORE INFORMATION, PLEASE CONTACT:

TODD INSKEEP
PRINCIPAL – COMMERCIAL STRATEGY
INSKEEP_TODD@BAH.COM
@TODD_INSKEEP