

# RSA® Conference 2019

San Francisco | March 4–8 | Moscone Center



# BETTER.

SESSION ID: PDAC-T06

## Rethinking Efficient Third-Party Risk Management

**Todd Inskeep**

Director

Booz | Allen | Hamilton

@Todd\_Inskeep

#RSAC



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

# So, what's driving 3<sup>rd</sup> 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 3<sup>rd</sup> party risk program is really two programs

## Your infosec program

Demonstrating how you manage risk  
as a 3<sup>rd</sup> party to other companies



## Your 3<sup>rd</sup> party program

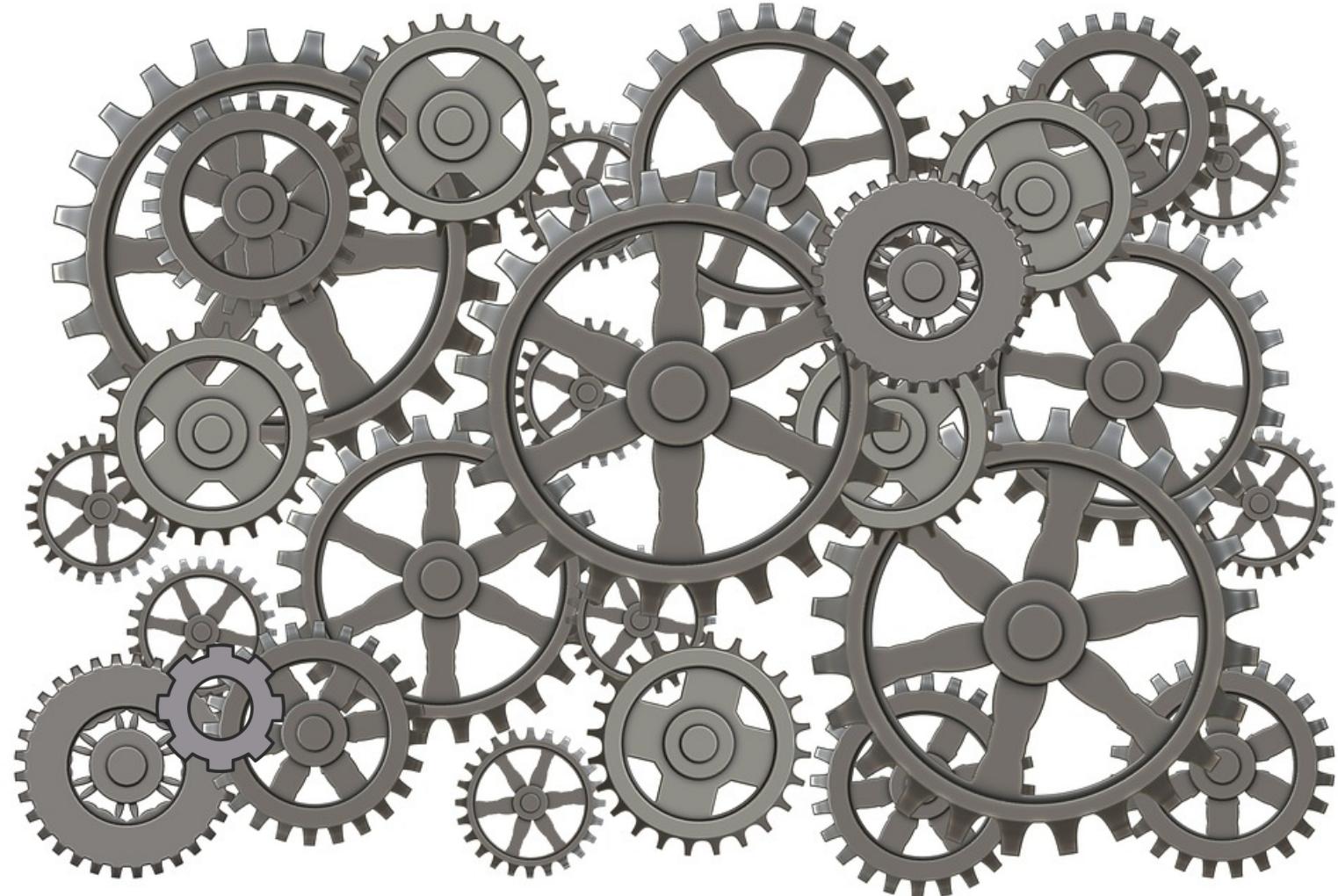
Managing risk from your 3<sup>rd</sup> parties



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

# Are you a Third party? Or managing third parties?

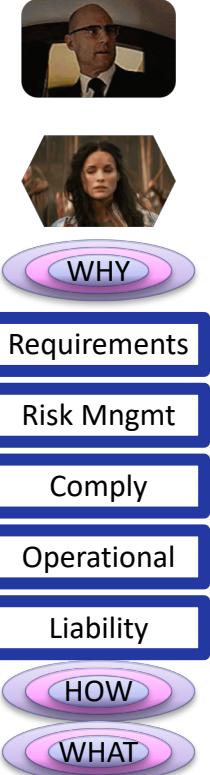
- You start off, the center of your universe...
- And pretty soon you can't find yourself



# 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

Four score and 7 weeks ago, our CISO brought forth a new Information Security Program, conceived in ISO 27001, and dedicated to meeting NIST CSF maturity. Now we are questioned whether this program, or any program so conceived and so dedicated can pass muster for a third party risk management program. We are met during an audit of that program. We have come to dedicate a large portion of our time to answering questions about the program, that our program, and our relationship with you, our customer, might long endure. Our brave team have struggled mightily to ensure the security of our systems. The world may little note, nor long remember the answers to these questions, we can only hope that our efforts are sufficient to protect us from adversaries.



# 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, 2013; Hong Kong Personal Data (Privacy) Ordinance; (vii) the Australia Privacy Act 1988; and (viii) the United States Gramm-Leach-Bliley Act of 1999.

"Remediation Efforts" means, with respect to any Security Incident, activities designed to remediate the nature of such Security Incident. Remediation Efforts may include: (A) development of new processes; (B) identification of affected individuals; (C) notification of affected individuals; (D) provision of identity theft insurance for affected individuals; (E) cooperation with law enforcement and other relevant parties in connection with litigation...

"Security Best Practices" means, as applicable, standards, requirements, specifications or obligations for information security, including (i) ISO 27001; (ii) NIST Cybersecurity Framework; (iii) SSAE 16, SOC 2 and SOC 3 auditing standards; (iv) Shared Services Center of Excellence.

"Security Incident" means, in connection with the Provider Systems or Services with respect to TheCompany, any unauthorized access, corruption, sale, rental, or destruction of such TheCompany's or Enterprise data or other breach which may stem from an act or omission to act) that would result in any of the events described above.

2. **Provider Warranties.**

(a) **Obligations toward Enterprises.** If Provider provides the Provider Services to TheCompany, then the following provisions shall apply:

- (i) **Compliance.**
- (ii) **Appropriate Safeguards.** Provider represents, warrants and covenants that it will implement appropriate safeguards to protect TheCompany's data in accordance with the applicable laws and regulations.
- (iii) **Evaluations.** Provider shall ensure that Provider Personnel are evaluated on a regular basis to determine their compliance with the applicable laws and regulations. The results of such evaluation, testing, and monitoring shall be provided to TheCompany.

(a) **Obligations toward TheCompany and Enterprises.** With respect to TheCompany and Enterprises, Provider represents, warrants and covenants that it will:

- (i) **Control.** Provider represents, warrants and covenants that it will have sole control over the data and will not share it with any third party without TheCompany's prior written consent.
- (ii) **Design.** Provider represents, warrants and covenants that it will design its systems and processes to ensure the security and integrity of TheCompany's data.
- (iii) **Notices.** Provider will provide TheCompany with prompt written notice of any security incident or breach that may affect TheCompany's data.

(b) **Security Reviews.** TheCompany (or its designated representatives) may request a review of all aspects of Provider's performance, including, but not limited to: (i) software development and testing; (ii) secure development requirements, test plans, code reviews, security audits; (iii) back-up procedures; (v) change and problem management processes and procedures; and (vi) Provider's obligations under this Agreement, in which case Provider will bear and reimburse TheCompany for the costs of such review.

(c) **Business Associate Agreement.** In the event that Provider creates, retains, or discloses TheCompany's data, Provider will enter into a Business Associate Agreement with TheCompany.

(d) **Security Incidents.**

- (i) **Remediation Efforts.** Provider will promptly notify TheCompany of any Security Incident until such Remediation Efforts have been implemented and tested for effectiveness and reasonableness. Provider will (i) at TheCompany's sole discretion, either undertake Remediation Efforts or engage a third party to do so, in which event (A) Provider must notify TheCompany in writing promptly after conclusion of such Remediation Efforts includes components aimed at preventing future incidents.
- (ii) **Notice to Enterprises.** Any notifications to Enterprises of Security Incidents will be made in accordance with the requirements set forth in this Agreement ("Business Continuity Plan").

(e) **Business Continuity.** Provider will at all times during the Term maintain a Business Continuity Plan that 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
- Often copied and pasted without regard to your specific products or services

# 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**

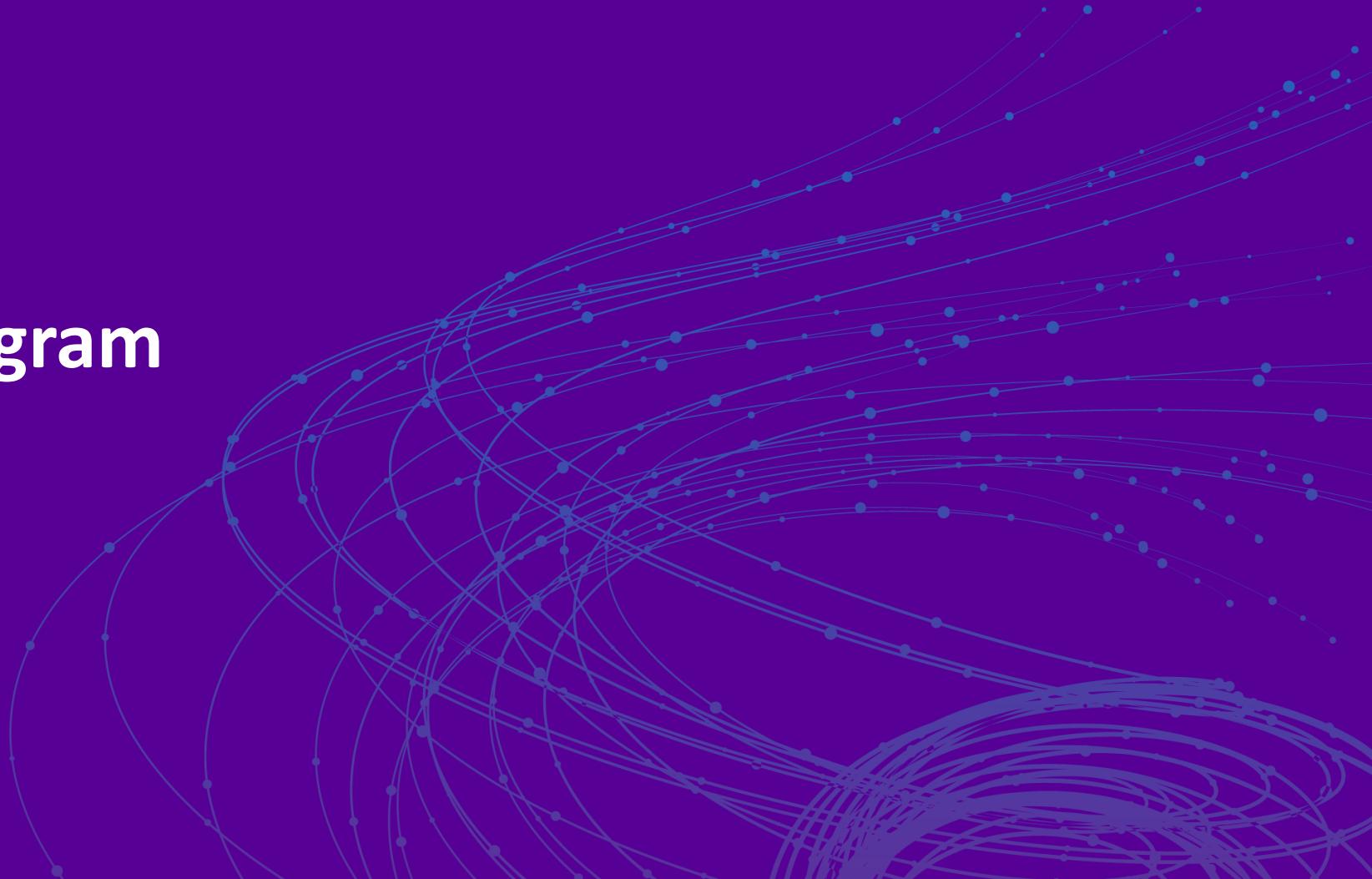
# Last thoughts on your information security program



- 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

# RSA® Conference 2019

## 3<sup>rd</sup> Party Program



# Forge your 3<sup>rd</sup> party program carefully



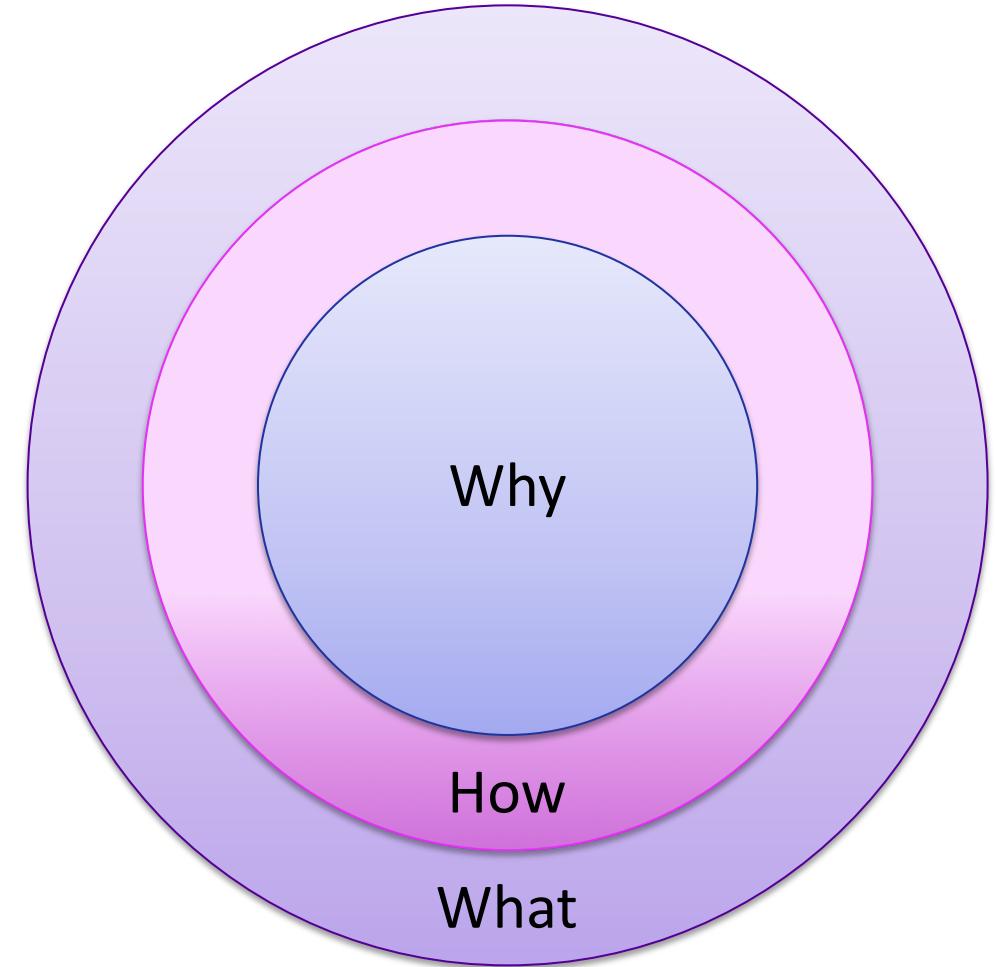
Optimize what drives your business success

Calibrate for  
Your company

Minimally do what you have to

# 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 3<sup>rd</sup> parties

Requirements

## 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, 2013; Hong Kong Personal Data (Privacy) Ordinance; (vii) the Australia Privacy Act 1988; and (viii) the U.S.

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

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

"Security Incident" means, in connection with the Provider Systems or Services with respect to 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 described below.

## 2. Provider Warranties.

(a) **Obligations toward Enterprises.** If Provider provides the Provider Services, the following warranties apply:

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

(i) **Compliance.**

(ii) **Appropriate Safeguards.** Provider represents, warrants and covenants that:

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

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

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

(ii) **Design.** Provider represents, warrants and covenants that:

including without limitation, secure development requirements, test plans, code reviews, security reviews, and security audits.

(iii) **Notices.** Provider will provide ~~TheCompany~~ with prompt written notice of any material change to the Services.

(b) **Security Reviews.** ~~TheCompany~~ (or its designated representatives) may conduct periodic reviews of the Services, including, but not limited to: (i) software design and development; (ii) back-up procedures; (v) change and problem management processes and procedures; and (vi) Provider's compliance with applicable laws and regulations.

(c) **Business Associate Agreement.** In the event that Provider creates, retains, or discloses any information relating to ~~TheCompany~~:

(d) **Security Incidents.**

(i) **Remediation Efforts.** Provider will promptly notify ~~TheCompany~~ of any Security Incident until such Remediation Efforts have been implemented and tested for effectiveness and reasonableness. Provider will (i) at ~~TheCompany~~'s sole discretion, either undertake Remediation Efforts or provide a plan to do so, or (ii) if the plan associated with such Remediation Efforts includes components aimed at preventing future incidents, provide a plan to do so.

(ii) **Notice to Enterprises.** Any notifications to Enterprises of Security Incidents will be made in accordance with the requirements set forth in this Agreement ("Business Continuity Plan").

(e) **Business Continuity.** Provider will at all times during the Term maintain Business Continuity Plan that 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

Risk Mngmt

## Kinds of 3<sup>rd</sup> party risk

Risk of a Breach

Compliance with  
Security Standards

Privacy Compliance

Secure Design

Reputational Risk

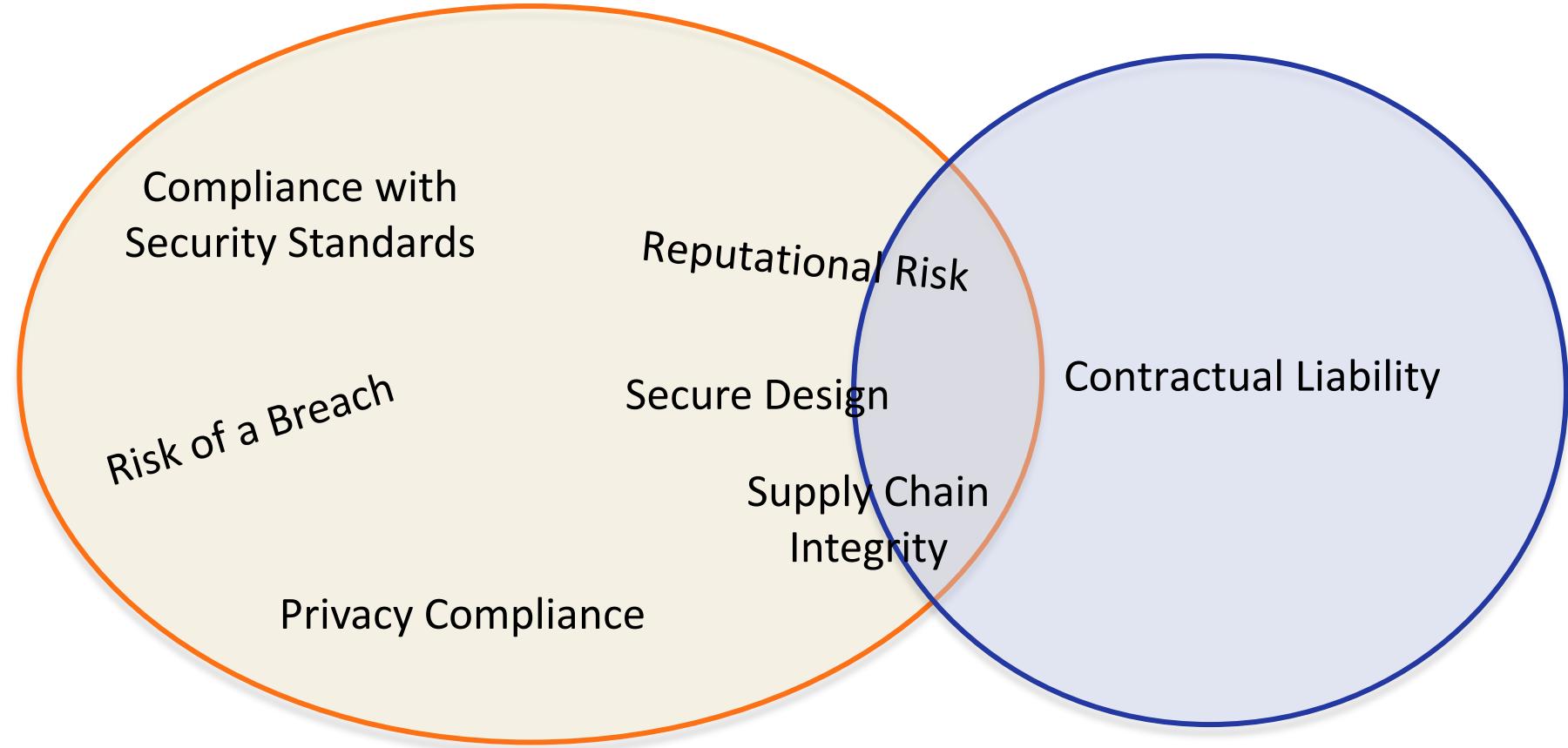
Contractual Liability

Supply Chain  
Integrity

# Manage risk from vendors

Risk Mngmt

## Kinds of 3<sup>rd</sup> party risk



- 3<sup>rd</sup> party risks we can control

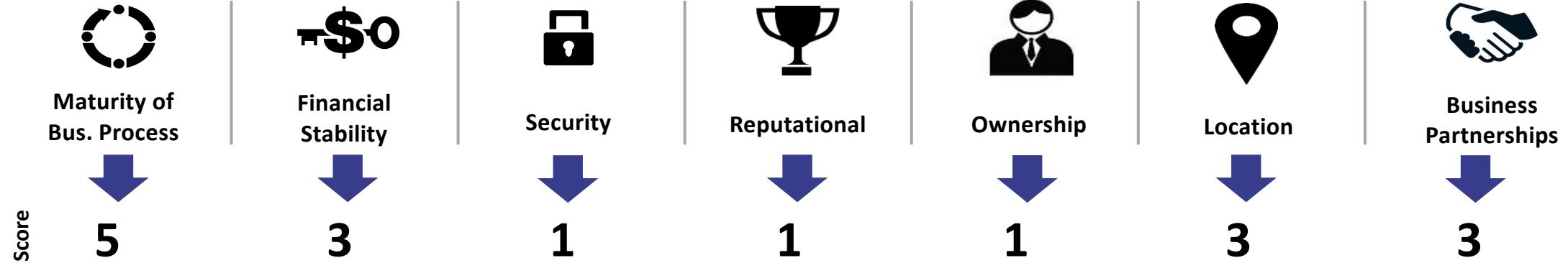
- 3<sup>rd</sup> party risks we can't control

# You can assess many kinds of risk from third parties

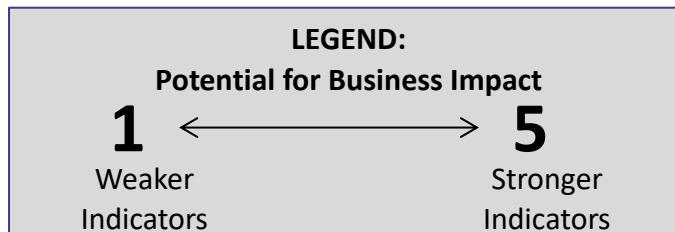
Risk Mngmt

ILLUSTRATIVE

## Supplier Risk Considerations



Score



**Assess the risks that concern  
your business the most**

# Complying with external requirements

Comply

## 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

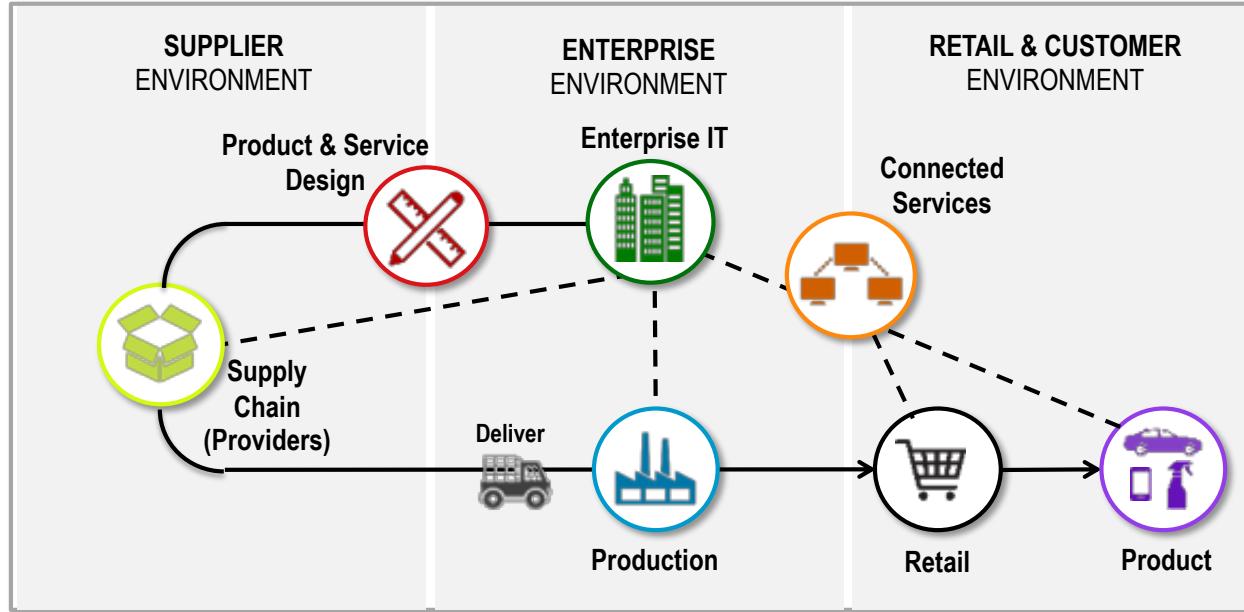
- Any third party that contacts PHI through the work it performs is a business associate, or BA.
- Both parties must have a contract detailing commitments to compliance
  - Providing assurances relating to the safeguarding of phi or the electronic equivalent, ephi
  - Before granting any level of access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

# Manage operational risk

Operational



- 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.

# Managing liability

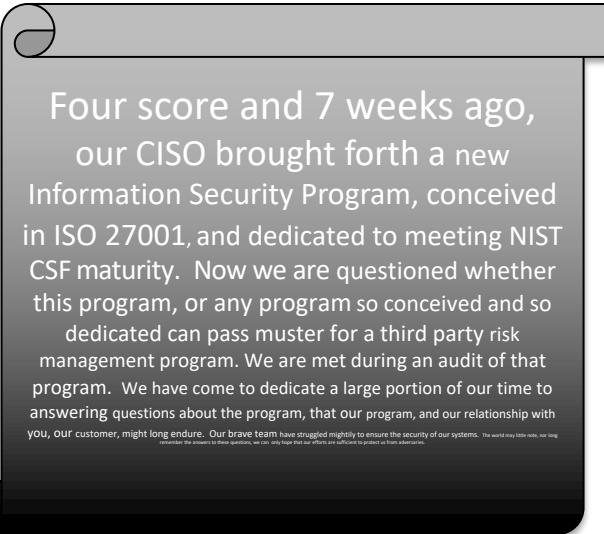
Liability

- 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

# Minimize most requests to suppliers

Liability

- 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?

# Standard approach to building a program

Phase	Phase 1: Initiate	Phase 2: Evaluate	Phase 3: Report	Future: Improve
Tasks	1a Build Program plan	2a Classify & prioritize vendors 2b Pilot vendor questionnaires 2c Pilot onsite audits	3a Review results 3b Determine investments 3c Manage issues	Maintain operations Mature capabilities Test & refine program
Activities	<ul style="list-style-type: none"> <li>• Program plan</li> <li>• Identify vendor classifications</li> <li>• Identify vendors</li> <li>• Establish security requirements</li> </ul>	<ul style="list-style-type: none"> <li>• Surge for initial activities</li> <li>• Establish priority classifications, and triage vendors against classification</li> <li>• Establish security requirements and test questions with various vendors</li> <li>• Determine audit approach and validate</li> <li>• Collect results and document processes</li> </ul>	<ul style="list-style-type: none"> <li>• Review initial program solutions</li> <li>• Identify options for investments to improve program</li> <li>• Manage issues; drop vendors if needed</li> </ul>	<ul style="list-style-type: none"> <li>• Get ongoing operations and align resources</li> <li>• Mature and optimize capabilities</li> <li>• Refine program with continuous review &amp; improvement</li> </ul>

# 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 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> party security. CISSP or similarly certified security experts combined with internal training on company risk processes, source selection, and contracting facilitates highly effective 3<sup>rd</sup> party risk management.
- Critical 3<sup>rd</sup> 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.

# 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

- |  |  |
|--|--|
| <ul style="list-style-type: none"> <li>• Agenda</li> </ul>   | <ul style="list-style-type: none"> <li>• Goals</li> </ul>  |
| <ul style="list-style-type: none"> <li>• Welcome Breakfast</li> <li>• Code of Conduct</li> <li>• Introduction to IT Leadership Team</li> <li>• Corporate Business &amp; Information Technology's Response           <ul style="list-style-type: none"> <li>— Commercial Business Challenges</li> <li>— Research &amp; Development</li> </ul> </li> </ul> | <ul style="list-style-type: none"> <li>• Manufacturing and Supply Chain</li> <li>• General &amp;Administrative</li> <li>• IT Portfolio &amp; Project Management</li> <li>• Information Security</li> <li>• Workshops</li> <li>• Closing Remarks/Q&amp;A</li> </ul> |
| <ul style="list-style-type: none"> <li>• Demonstrate shared values</li> <li>• Identify additional business opportunities</li> <li>• Develop partnerships</li> <li>• Know your counterparts</li> </ul>  |  |

# So, What?

## What do you spend effort on to be efficient??

WHAT

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

WHAT

- Prioritizing 3<sup>rd</sup> party risk and security management against competing security program portfolio activities and priorities
- Automation tools for 3<sup>rd</sup> 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 3<sup>rd</sup> parties, similar needs
  - Reduce system noise and turbulence
  - Highlight opportunities to work together
  - Drive the right behaviors

**"Useful Tool, If It Didn't Account For False Positives"**

 Overall User Rating

Product(s): XYZ Platform

Overall Comment: "XYZ Platform is an interesting tool in its own right, but certainly not without any faults. After working with several vendors, it was determined that many of the findings weren't reviewed by the vendor before being made present to myself or other members of the team. Additionally, there is a high false positive rate for many of the findings, which adds further confusion and frustration when evaluating third party vendors."

Source: Gartner Peer Insights™

# Apply these lessons at home

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

# QUESTIONS



Thank You

FOR MORE INFORMATION, PLEASE CONTACT:

TODD INSKEEP  
PRINCIPAL – COMMERCIAL STRATEGY

[INSKEEP\\_TODD@BAH.COM](mailto:INSKEEP_TODD@BAH.COM)

@TODD\_INSKEEP