Vendor Security Checklist

□ 1. Identify Supply Chain Exposure

What Vendors do you currently have? Check your Contract Management System (CMS), Enterprise Resource Planning (ERP), or Configuration Management Database (CMDB) for a starting point to create your Vendor Inventory.

□ 2. Categorize Vendor Services

Using your inventory & categorized vendor services, what needs security consideration? Ex. SaaS Security, Self-Hosted Third-Party solutions, SaaS Contracts, Outsourcing Contracts, Consulting Contracts, etc.

□ 3. Program Scoping

Using your categories, select what needs security consideration. Ex. SaaS, Self-Hosted third Party solutions, SaaS Contracts, Outsourcing Contracts, Consulting Contracts, etc.

□ 4. Tiering Methodology

Your program scope may consist of hundreds of vendors but do all of these need the same level of security diligence? Probably not, this is why you would tier your vendor relationships. Tiering is the process of creating a formula to determine the how sensitive a vendor is your company. The more sensitive the tier, the more diligence you perform on a more frequent basis.

Be sure to clearly define the actions or strategies associated with each tier. Example:

A. Strategic Partners: Collaborate closely, engage in joint planning, and explore long-term relationships.
B. Critical Suppliers: Monitor closely, implement contingency plans, and conduct regular performance reviews.
C. Standard Suppliers: Focus on transactional relationships, with routine monitoring and periodic evaluations.

□ 5. Policy Development

With the data you've collected you now have what you need to establish your policy. Your policy will give your program the foundation and authority to operate within your organization. Considering including things such as tiering needs, evaluation frequency, contract requirements, etc.

□ 6. Operationalization Planning

Program effectiveness is key for success. After all, you can't protect what you can't see. How will you make sure when something is being purchased that you're embedded in the procurement process (RFI/RFPs) early enough to advise your business partners on strategic IT purchases and conduct your evaluation without hurting business velocity? Find the entry point for purchasing and insert your starting point there.

Hint. Legal is a great partner who has the same need and can help. Legal can also help with security language in contract.

Vendor Security Checklist Continued

☐ 7. Draft Process

Diagram the process and highlight your key contributors (legal, business (stakeholders and product owners), vendor, etc.)

☐ 8. Leadership Approval

Obtain leadership buy-in from your security & business leadership for what you're evaluating and the criteria to determine vendor criticality. Vendor relationships may be sensitive and leadership support will be needed when something bad is found, someone complains, or escalation support is needed.

☐ 9. Technology Support

What will be used to operationalize this program? Starting with excel docs, sharepoint, and email is very common but will become frustrating rather quickly. A dedicated vendor security solution may not be in the budget so look at what's already in house.

Hint. Airtable, Smartsheets, etc.

☐ 10. Contract Language Development

Partner with your legal team to develop contract language to hits on your security needs. It's better to get your criteria down on paper and have your legal team draft the final version. Ex. IR notification criteria, data usage clauses, regulatory compliance, data residency needs, termination clauses, SLA requirements & penalties, etc.

☐ 11. Questionnaire Development

What do you want to make sure your vendors are doing? This is a challenging step. You'll want to make sure your vendors have everything but that's not the goal, the goal is to have enough to make a risk informed decision. Identify if a certificate is within your risk tolerance (SOC2, ISO 27001, etc.) or if you need a questionnaire. If you need a questionnaire, be mindful that commonly available questionnaires like the SIG & CAIQ are several hundred questions and many may not be what you need. Contextualize the vendor questionnaire to avoid vendor fatigue and provide background information to set the stage to ensure that vendors understand the purpose and context of the inquiry.

☐ 12. Risk Management

What are you going to do with the issues you find? If you have a risk management program plug into it otherwise you may need to create tracking and escalation procedures.