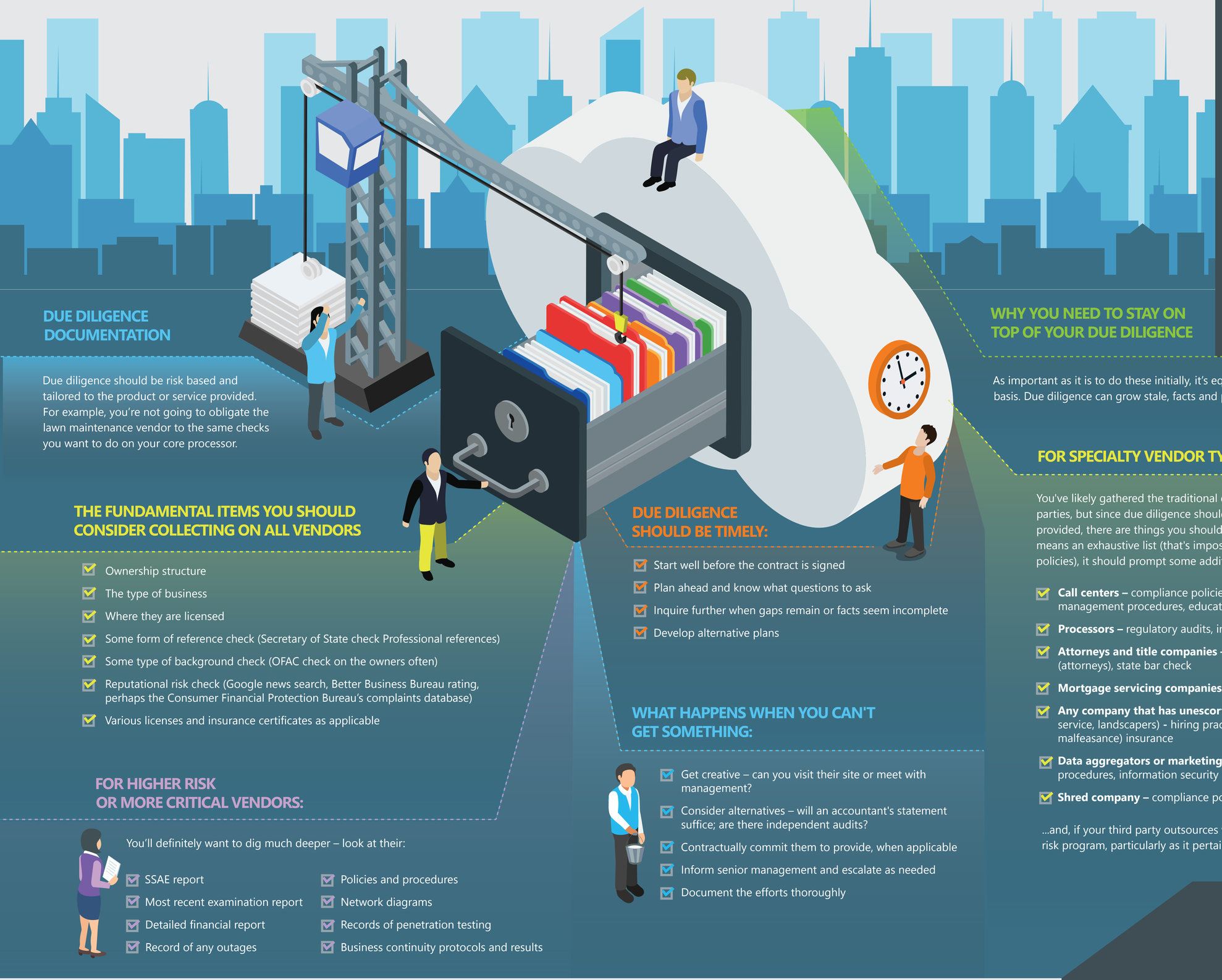
Vendor + Product + Risk = Documentation

What due diligence documents should you be requiring based on risk?

Understanding the basics of the vendor with whom you are planning to do business is a fundamental requirement of all of the regulatory guidance. More importantly, it's just a good business practices and good ol' common sense.

You likely get recommendations on whom you choose to service your car, do a little background on the doctor you're selecting… those are elements of due diligence in your personal life, but you should use a very similar approach in how you approach vendor due diligence.



DUE DILIGENCE DOCUMENTATION

Due diligence should be risk based and tailored to the product or service provided. For example, you're not going to obligate the lawn maintenance vendor to the same checks you want to do on your core processor.

THE FUNDAMENTAL ITEMS YOU SHOULD CONSIDER COLLECTING ON ALL VENDORS

- Ownership structure
- The type of business
- Where they are licensed
- Some form of reference check (Secretary of State check Professional references)
- Some type of background check (OFAC check on the owners often)
- Reputational risk check (Google news search, Better Business Bureau rating, perhaps the Consumer Financial Protection Bureau's complaints database)
- Various licenses and insurance certificates as applicable

FOR HIGHER RISK OR MORE CRITICAL VENDORS:

You'll definitely want to dig much deeper – look at their:

- SSAE report
- Most recent examination report
- Detailed financial report
- Record of any outages
- Policies and procedures
- Network diagrams
- Records of penetration testing
- Business continuity protocols and results

DUE DILIGENCE SHOULD BE TIMELY:

- Start well before the contract is signed
- Plan ahead and know what questions to ask
- Inquire further when gaps remain or facts seem incomplete
- Develop alternative plans

WHAT HAPPENS WHEN YOU CAN'T GET SOMETHING:

- Get creative – can you visit their site or meet with management?
- Consider alternatives – will an accountant's statement suffice; are there independent audits?
- Contractually commit them to provide, when applicable
- Inform senior management and escalate as needed
- Document the efforts thoroughly

A NOTE FROM CHIEF RISK OFFICER, BRANAN COOPER

Many companies have a detailed spreadsheet of what they require from each type of vendor and the frequency with which they gather it. Personal preference – I find these to be too strict and by trying to define into a pigeon hole, you may forget the fundamental step of making sure that the due diligence is relevant, applicable, common sense and appropriate…and, most importantly, tailored to the risk, not just the function performed.

In my presentations, I describe due diligence as a science and an art – there are always required steps, but there is a great deal to the presentation and interpretation as well. Due diligence is fundamentally important to you and to your third party.

WHY YOU NEED TO STAY ON TOP OF YOUR DUE DILIGENCE

As important as it is to do these initially, it's equally important to do them regularly on a scheduled and consistent basis. Due diligence can grow stale, facts and performance can change and you must stay on top of it.

FOR SPECIALTY VENDOR TYPES:

You've likely gathered the traditional due diligence items for all of your critical and / or high risk third parties, but since due diligence should be both risk based and tailored to the product or service provided, there are things you should still consider for particular third parties. While this is by no means an exhaustive list (that's impossible – you need to consider your institution's needs and policies), it should prompt some additional steps on your part.

- **Call centers –** compliance policies and procedures, hiring practices and background checks, change management procedures, education schedule
- **Processors –** regulatory audits, internal audits, quality assurance reports
- **Attorneys and title companies –** information security procedures, Martindale Hubbel checks (attorneys), state bar check
- **Mortgage servicing companies –** compliance policies and procedures, internal audits
- **Any company that has unescorted access to your building** (e.g. landlord, shred company, cleaning service, landscapers) **-** hiring practices and background checks, general liability (especially employee malfeasance) insurance
- **Data aggregators or marketing leads –** record retention policies, compliance policies and procedures, information security procedures
- **Shred company –** compliance policies and procedures, hiring practices and background checks

…and, if your third party outsources work to offshore vendors, take a close look at their third party risk program, particularly as it pertains to the masking of US customer data and record retention.

venminder

400 Ring Road, Suite 131, Elizabethtown, KY 42701 | (270) 506-5140
www.venminder.com

PRINTABLE VERSION