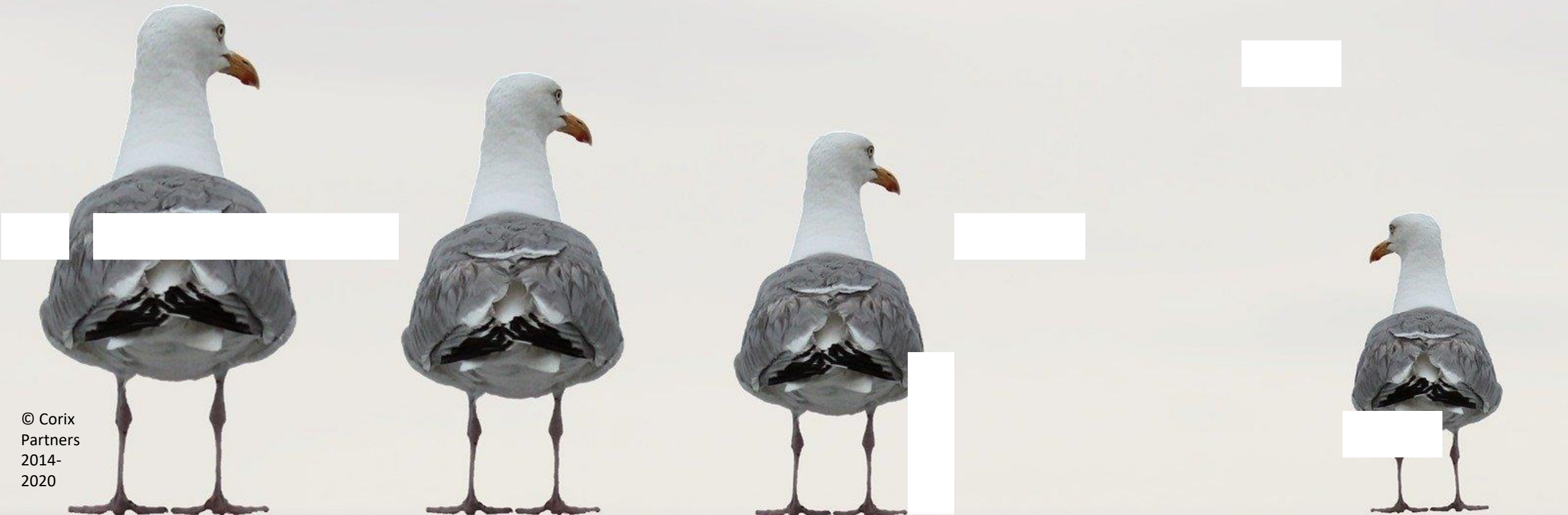
# Building a Vendor Risk Management Practice that Delivers Real Value

corix partners

## A Guide for Programme Managers

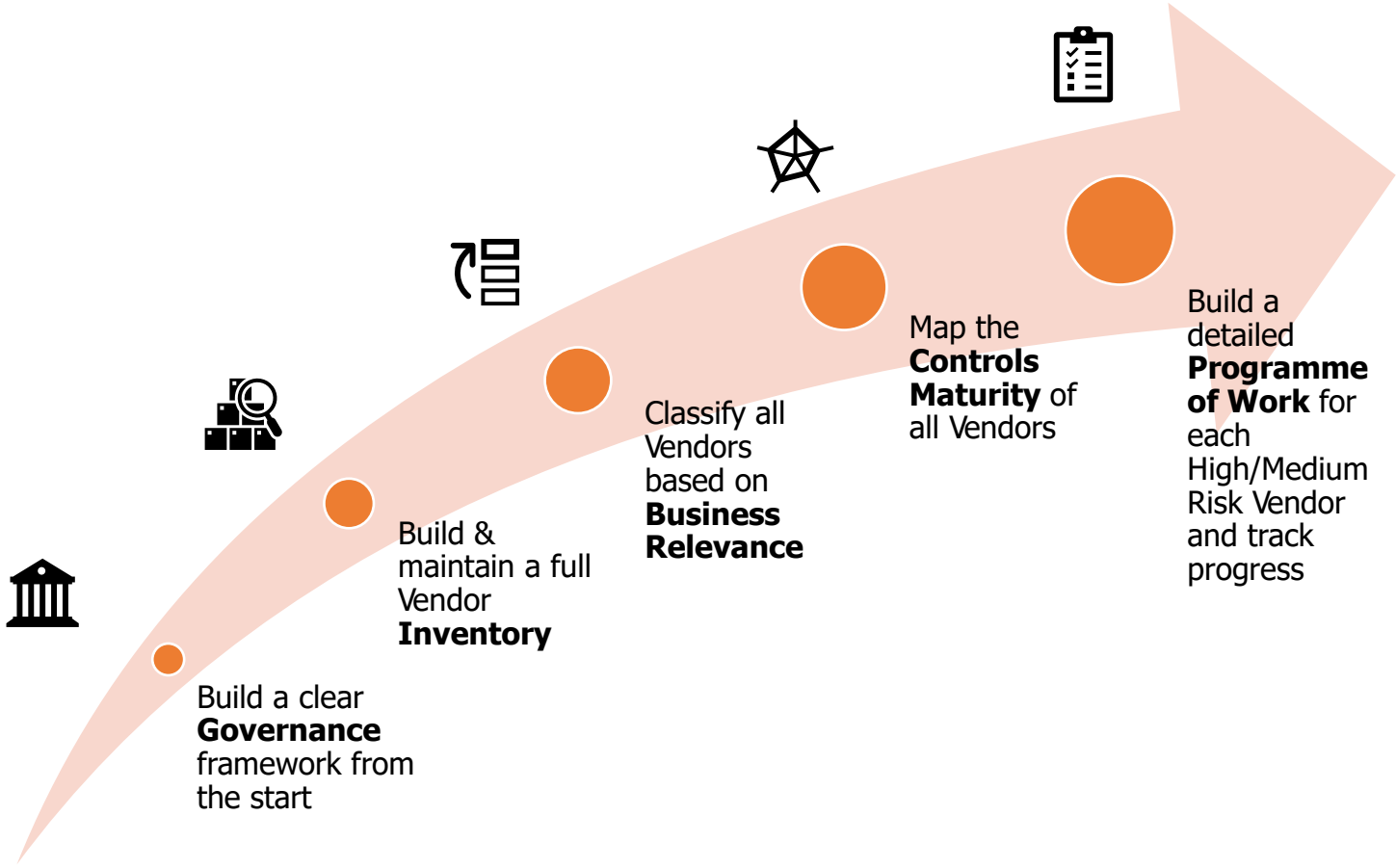


© Corix Partners 2014-2020

# 5 Steps to Building a Vendor Risk Management Practice

***Keep Things Simple:***

*This is about, identifying whether Vendors have or don't have the right Controls in place to protect your Business and driving remedial actions where needed*




Focus on Controls and on agreeing and tracking remedial actions with key Vendors

© Corix Partners 2014-2020

# Build a Clear Governance Framework from the Start

*You need to understand from the start where the expectations are, and where the constraints will be for the exercise*

### Why are you doing this?

- Understand upfront what management objectives really are: Audit/regulatory "tick- in-a-box" with a few Vendors perceived as critical, vs. genuine broad controls interest;
- Based on that, you may have to look for “quick wins” as well as putting in place a broader programme of work;
- Understand the degree of formality the process needs to have (or not)

### Where should your focus be?

- “Vendors” are very diverse and the word itself means different things to different people;
- Business approach vs. IT approach: Is this all (just) about “the Cloud?”
- What about geographies or business lines? How independent are they with Vendors selection?


### Who are you working for on this?

- Reporting lines?
- Understand upfront how unsatisfactory outcome (“high risk Vendor” situations or lack of cooperation) will be handled, and by whom

### What is this leading to and where is this feeding into?

- Reporting frequencies, reporting formats?
- What output is expected of you?
- Schedule periodic meetings from the start so that progress can get tracked

Ensure that you have the right amount of resources and commitment from the start and manage expectations upstream to cope with delays, lack of cooperation and internal politics down the line

© Corix Partners 2014-2020

# Build and Maintain a full Vendor Inventory

*Don't be scared by the size of the inventory, but make sure you right-size your own practice*


Make sure that you have the right amount of resources to deliver your programme of work over the right timeframes: Do not become a bottleneck in your own practice.

© Corix Partners 2014-2020

# Build and Maintain a full Vendor Inventory

***Context is Key:***

*You will need to operate within the frame of the established relationship with each Vendor*

- For each Vendor, ensure you have a clear understanding about who owns the relationship internally and on the Vendor side
    - You need to establish a relationship owner for each Vendor, and a simple set of activities and responsibilities in relation to the role.
- Ensure you have a clear understanding of the Vendors with whom the relationship is already damaged
    - And a high level understanding of the problems (where relevant).
- Ensure you have a clear understanding of your actual legal position in all cases
    - Do you have a contractual “right-to-audit” with each Vendor?
    - Does the “right-to-audit” have any relevant limitations?
    - What are you contractually asking Vendors to adhere to? (e.g. industry good practices)

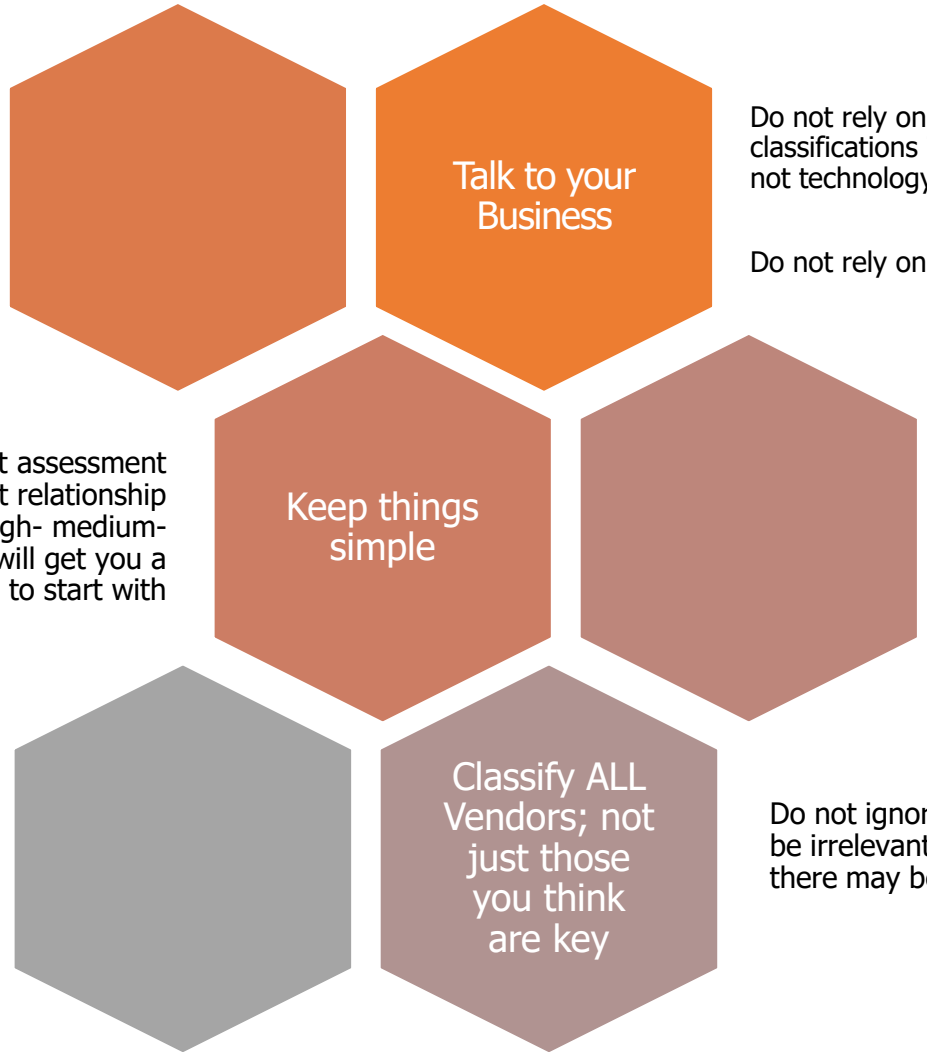
Make sure you build a simple process with the right control points with all stakeholders to ensure your inventory remains up to date

© Corix Partners 2014-2020

# Classify all Vendors based on Business Relevance

***Prioritisation is Key:***

*Not all Vendors have the same importance to a given business process;*
*Not all business processes have the same importance to the business as a whole;*
*And all this may vary over time*




Do not rely only on IT or BCP classifications if they exist (process first, not technology)

Do not rely only on Contract Value

A basic impact assessment with the right relationship owner and a high- medium- low ranking will get you a long way to start with

Do not ignore those which appear to be irrelevant (e.g. websites etc…); there may be surprises…

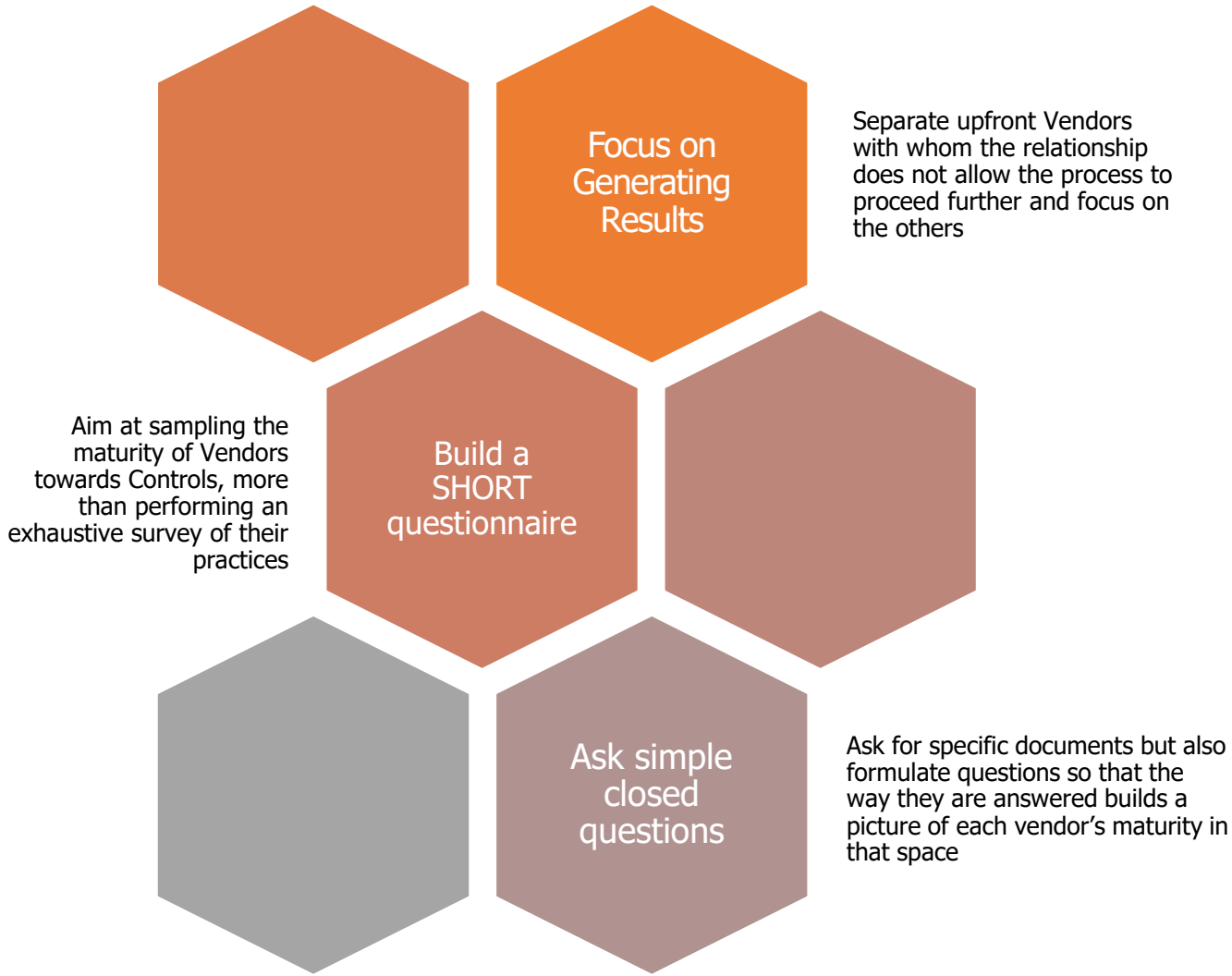
Make sure you build a simple process with the right control points with Procurement, Legal, HR, IT and the Business to periodically review these ratings.

© Corix Partners 2014-2020

# Map the Controls Maturity of all Vendors

***Simplicity is Key:***

*Complex approaches alienate Vendors and do not bring results*




Do not over-engineer the overall approach: Focus on producing results and avoiding pushback from Vendors

© Corix Partners 2014-2020

# Map the Controls Maturity of all Vendors

***Be Realistic:***

*Vendors are inundated by requests like yours and you will never get full access to their operating environment*

- Validate the approach with each relationship owner THEN send the short questionnaire to the Vendors
  - You may have to proceed in phases in the event too many relationship owners want to delay the process.
- Give a realistic but strict deadline for completing the questionnaire
  - Present it as a high level survey;
  - Do not enter into any detailed direct discussion with any particular Vendor at this stage;
  - Make sure all Vendors have the same level of information.
- Factor attitude towards the survey in your maturity assessment
  - Vendors sending the wrong documents, providing vague answers or brochureware, not answering questions (practically or effectively), not answering at all, should all be marked down.

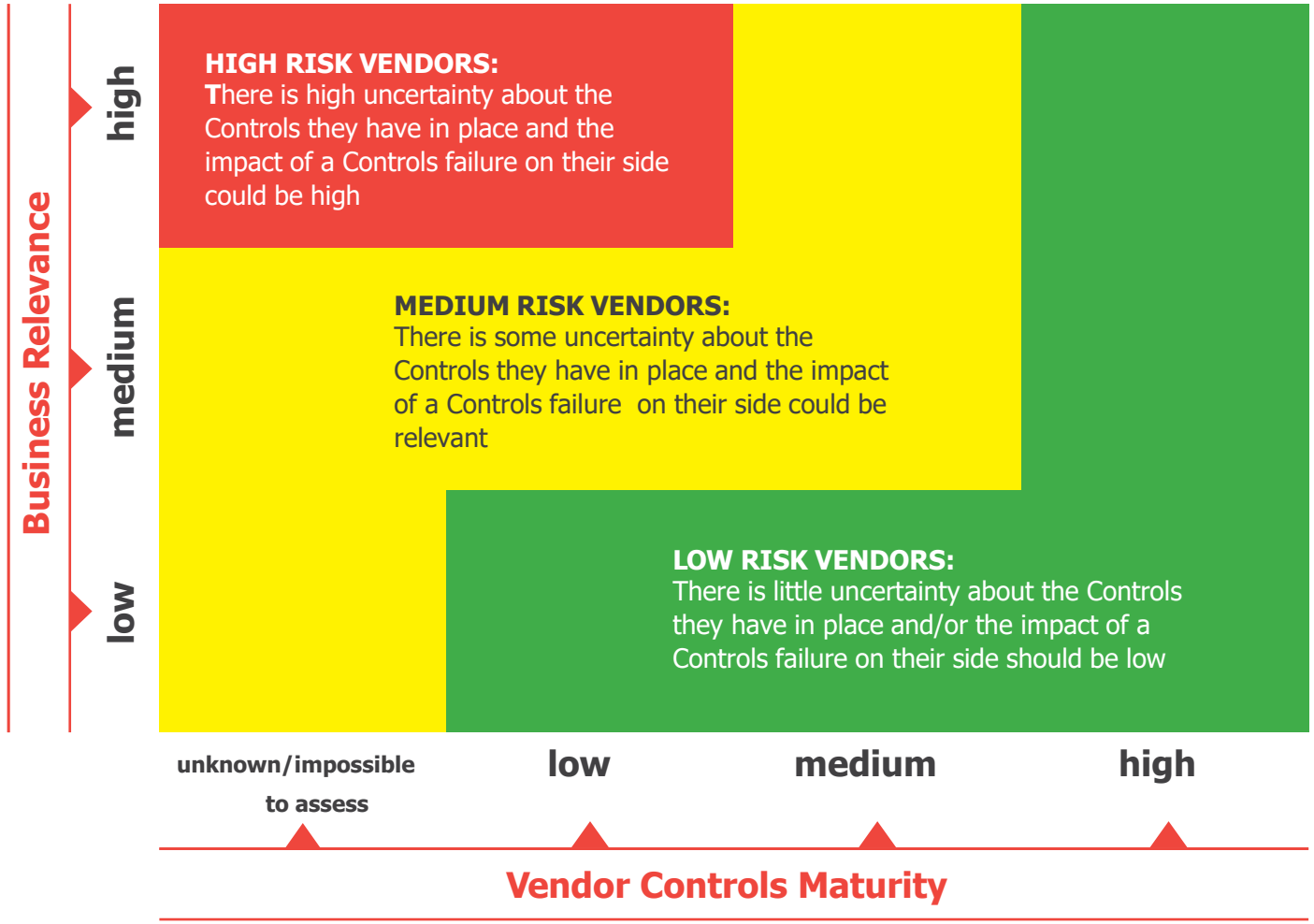
Be patient as collecting the right information may take time, and build on managed expectations with senior stakeholders internally

© Corix Partners 2014-2020

# Map the Controls Maturity of all Vendors

***The Risk Interpretation:***

*Map results into a matrix for reporting & decision making purposes and use it to determine next steps.*

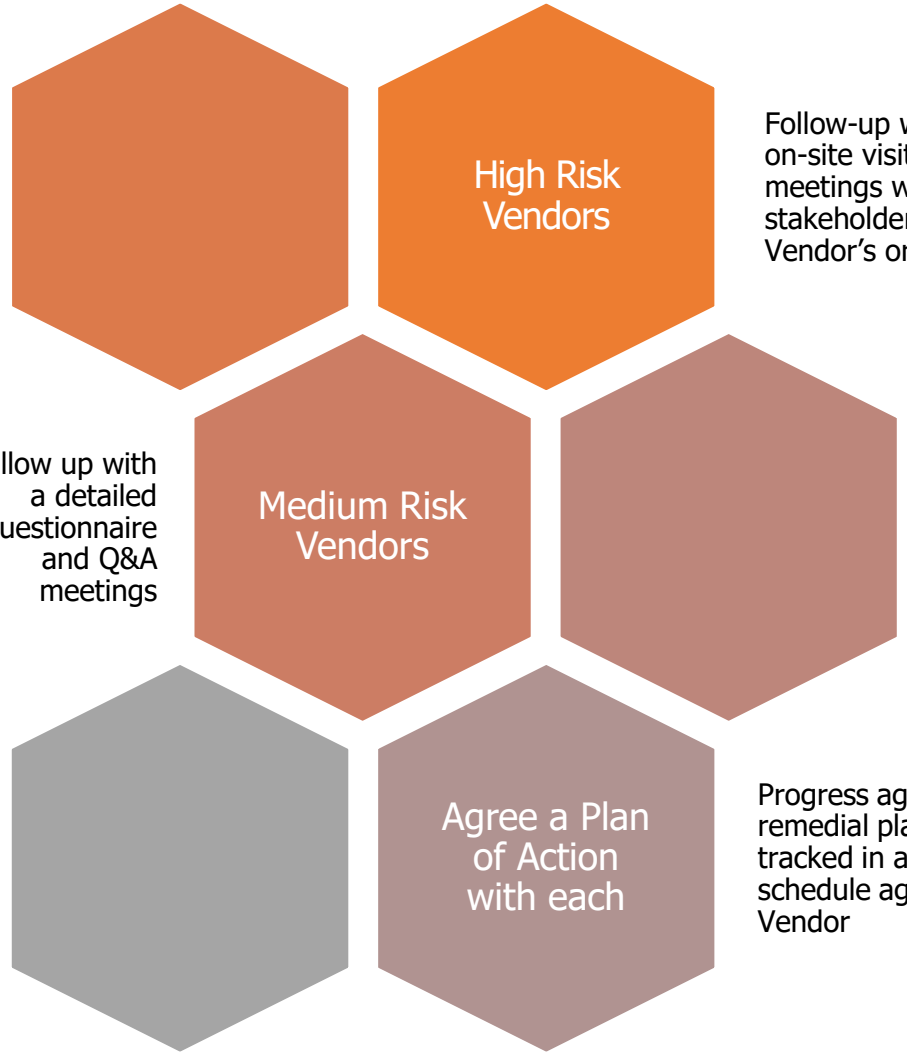



The key objective is to be able to focus quickly on **high** Business Relevance Vendors with **low** (or unknown) Controls Maturity

© Corix Partners 2014-2020

# Build a Detailed Programme of Work for each High/Medium Risk Vendor and Track Progress

*Ensure each step is validated with each relationship owner and scheduled over a relevant period of time, based on resources available on your side and with the Vendors*

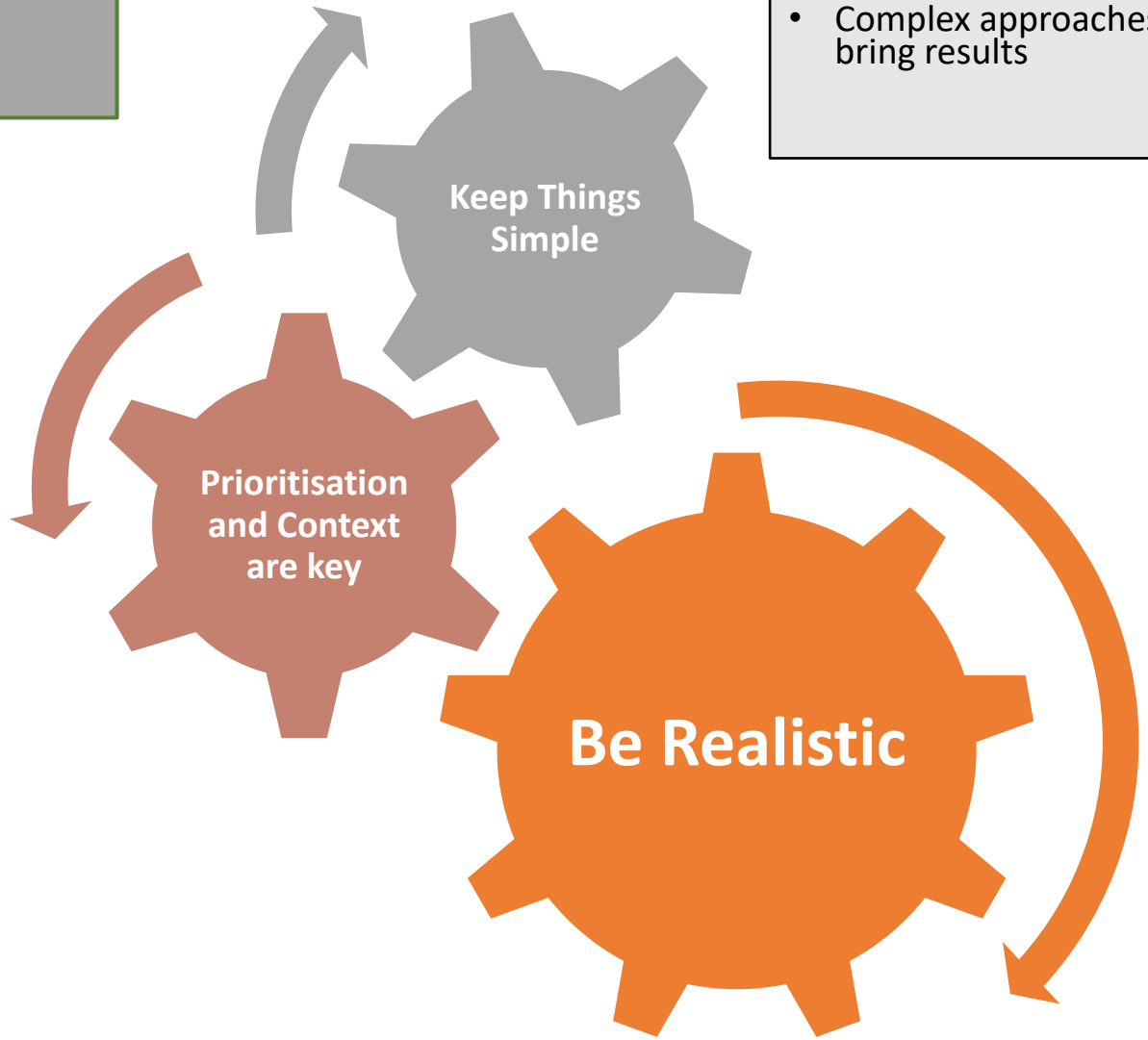



Avoid conflicts and seek a compromise with each Vendor on the rightsizing of the exercise but stay firm: Report uncooperative Vendors to senior stakeholders internally and consider formal or legal action where necessary.

© Corix Partners 2014-2020

# Summary of Key Points

- This is about, identifying whether Vendors have or don't have the right Controls in place to protect your Business and driving remedial actions where needed
- Complex approaches alienate Vendors and do not bring results




- You will need to operate within the frame of the established relationship with each Vendor
- You will need to focus your limited resources on going behind the curtains with key Vendors
- Avoid conflicts and seek a compromise with each Vendor on the rightsizing of the exercise but stay firm: Report uncooperative Vendors to senior stakeholders internally and consider formal or legal action where necessary

- Vendors are inundated by requests like yours and you will never get full access to their operating environment
- The key objective is to be able to focus quickly on high Business Relevance Vendors with low (or unknown) Controls Maturity and drive a meaningful action plan with each

# Cyber Security: Not just an Equation between Risk Appetite, Compliance and Costs


269 Farnborough Road
Farnborough, Hampshire
GU14 7LY
United Kingdom



Registered in England and Wales
Corix Partners Limited (No. 06774109)

*Originally drafted in November 2014 and first published on the Corix Partners website in February 2015*


Please be in touch to discuss further


jcgaillard@corixpartners.com

+44 (0) 7733 001 530

www.corixpartners.com

@Corix_JC

@CorixPartners


Thank You


© Corix Partners
2014-2020