Building a Vendor Risk Management practice that delivers real value

A guide for Programme Managers

corix partners

Don’t focus on Risk; focus on Controls and on agreeing and tracking remedial actions with key Vendors

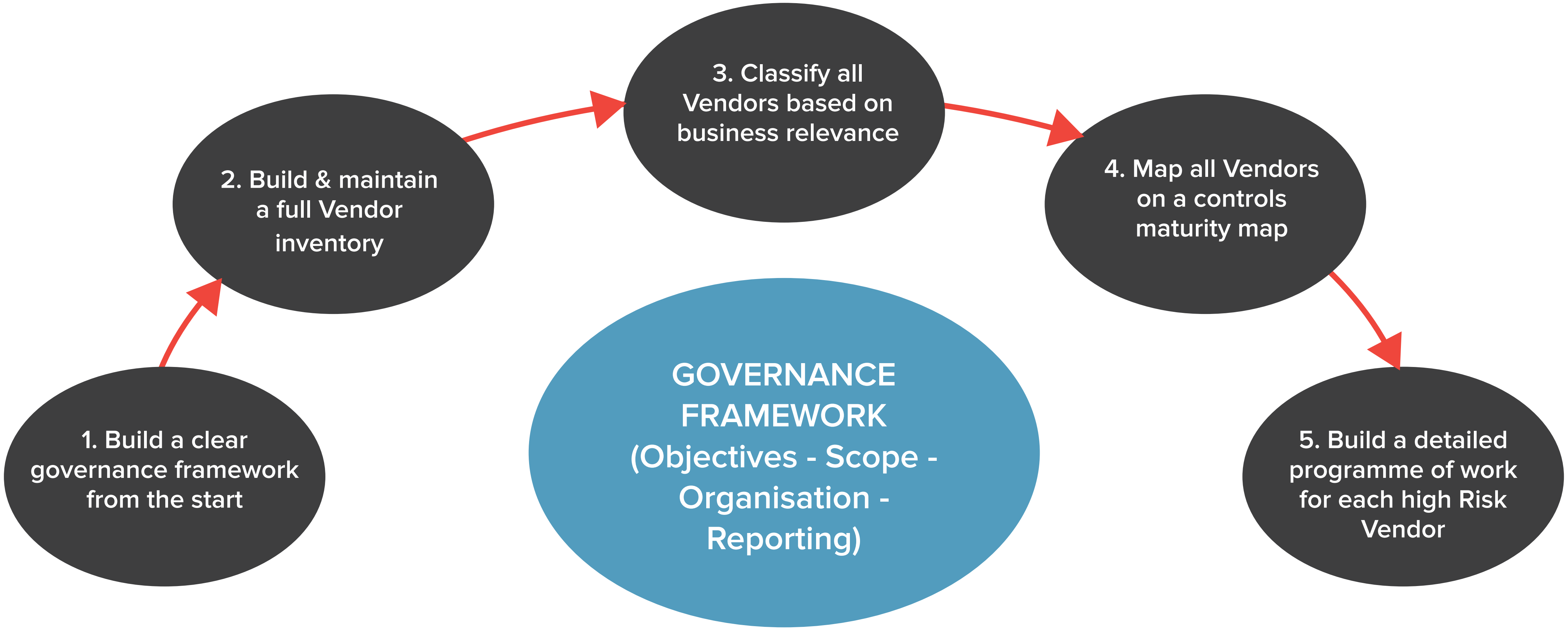
- Do not get into the wrong debate about what “Risk Management” is about (methodologies, integration with other Risk practices, etc…)

- Simply focus on Controls instead

- This is about Vendors having the right Controls in place (or not), and you identifying Controls deficiencies and driving remedial actions

- Focus Vendors on the reality of their Controls environment (and their contractual obligation), instead of an hypothetical discussion on what could go wrong

5 steps to building a Vendor Risk Management practise



1. Build a clear governance framework from the start

2. Build & maintain a full Vendor inventory

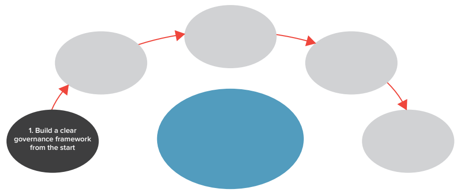
3. Classify all Vendors based on business relevance

4. Map all Vendors on a controls maturity map

5. Build a detailed programme of work for each high Risk Vendor

GOVERNANCE FRAMEWORK (Objectives - Scope - Organisation - Reporting)

1. Build a clear Governance framework from the start



Objectives

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)

Scope

“Vendor” means different things to different people

– “Vendors” are very diverse: Where should you focus first?

– Business approach vs. IT approach; is this all (just) about “the Cloud?”

Organisation

Who do you work for on this?

– Reporting lines?

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

Reporting

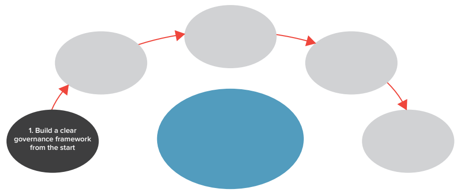
What is this leading to and where is this feeding to?

– Reporting frequencies, reporting formats?

– What output is expected of you?

– Schedule periodic meetings from the start so that progress can get tracked

1. Build a clear Governance framework from the start



Manage expectations upfront

- – You are going to get delays, unwillingness to participate, vague answers, generic answers, brochureware, etc.;
- – You are not likely to ever have full access to the Vendor environment;
- – You will have to make assumptions based on trust or distrust; this is hard to get right and takes time.

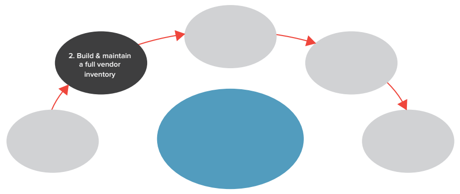
Prioritisation is key

- – YOU need to focus YOUR limited resources on going behind the curtains with key Vendors.

As much as realistically possible, ensure that you have the right amount of resources and commitment upfront

- – This is hard to get right and takes time.

2. Build and maintain a full Vendor inventory



Start with procurement and legal, but find ways of engaging with HR, IT and the business directly.

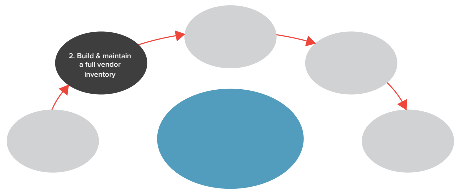
Assume that established procurement procedures would have been bypassed, so “look behind the curtains”.

Think process first, not technology; group Vendors by business process.

When it comes to technology, think structured as well as unstructured relationships (e.g. websites etc …)

- **Ensure you have a clear understanding about who owns the relationship internally and on the Vendor side;**
  - – You need 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.

2. Build and maintain a full Vendor inventory

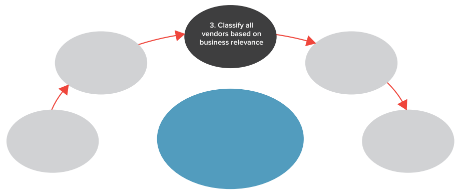


- **Ensure you have a clear understanding of your actual legal position in all cases**
  - – Do you have a contractual “right-to-audit” with each Vendor?
  - – Does the “right-to-audit” have any relevant limitations?
  - – What are you contractually asking Vendors to adhere to? (e.g. industry good practices)

- **Don’t be afraid about the size of the inventory, but make sure you rightsize 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.

- **Make sure you build a simple process with the right control points with all stakeholders to ensure your inventory remains up to date**
  - – Don’t forget HR; they are often the first (and worst) offender …

3. Classify all Vendors based on business relevance



- **Not all Vendors have the same importance to a given business process;**

  – and not all business processes have the same importance to the business as a whole;
  – and all this may vary over time;

- **Think process integrity, not Information sensitivity or system criticality.**

Talk to your business to understand this;

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

Do NOT rely on contract value.

Keep things simple and make sure you do this with the right relationship owner;

A basic impact assessment and a high-medium-low ranking will get you a long way to start with.

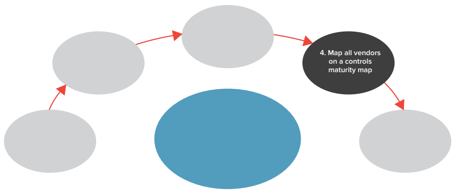
Classify ALL Vendors; not just those you think are key.

Do not ignore those that you believe are irrelevant (e.g. websites etc...);

There may be surprises...

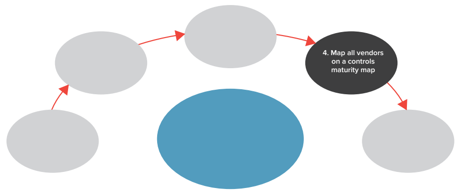
Make sure you build a simple process with the right control points with procurement, legal, HR, IT and the business to periodically review these ratings.

4. Map all Vendors on a controls maturity map



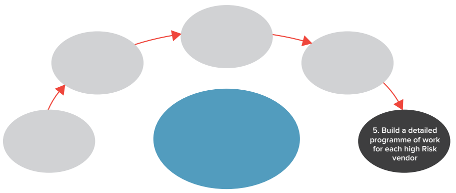
- **Separate up front Vendors with whom the relationship does not allow the process to proceed further (e.g. because it is perceived it would damage the relationship further);**
  - Their controls maturity will be ultimately classified as “Unknown” (see below).
- **Build a SHORT questionnaire aimed at sampling the maturity of Vendors towards controls;**
  - 15 controls max for high business relevance Vendors; fewer for lesser categories;
  - Controls to be taken out of existing internal policies and/or industry good / best practices and to be regarded as an undisputable baseline.
- **Ask simple closed questions and ask for specific documents;**
  - e.g. How many staff have you got in your Information Security function? Please provide an org chart for your Information Security function
  - Questions to be formulated so that the way they are answered builds a picture of the vendor’s maturity in that space

4. Map all vendors on a Controls maturity map

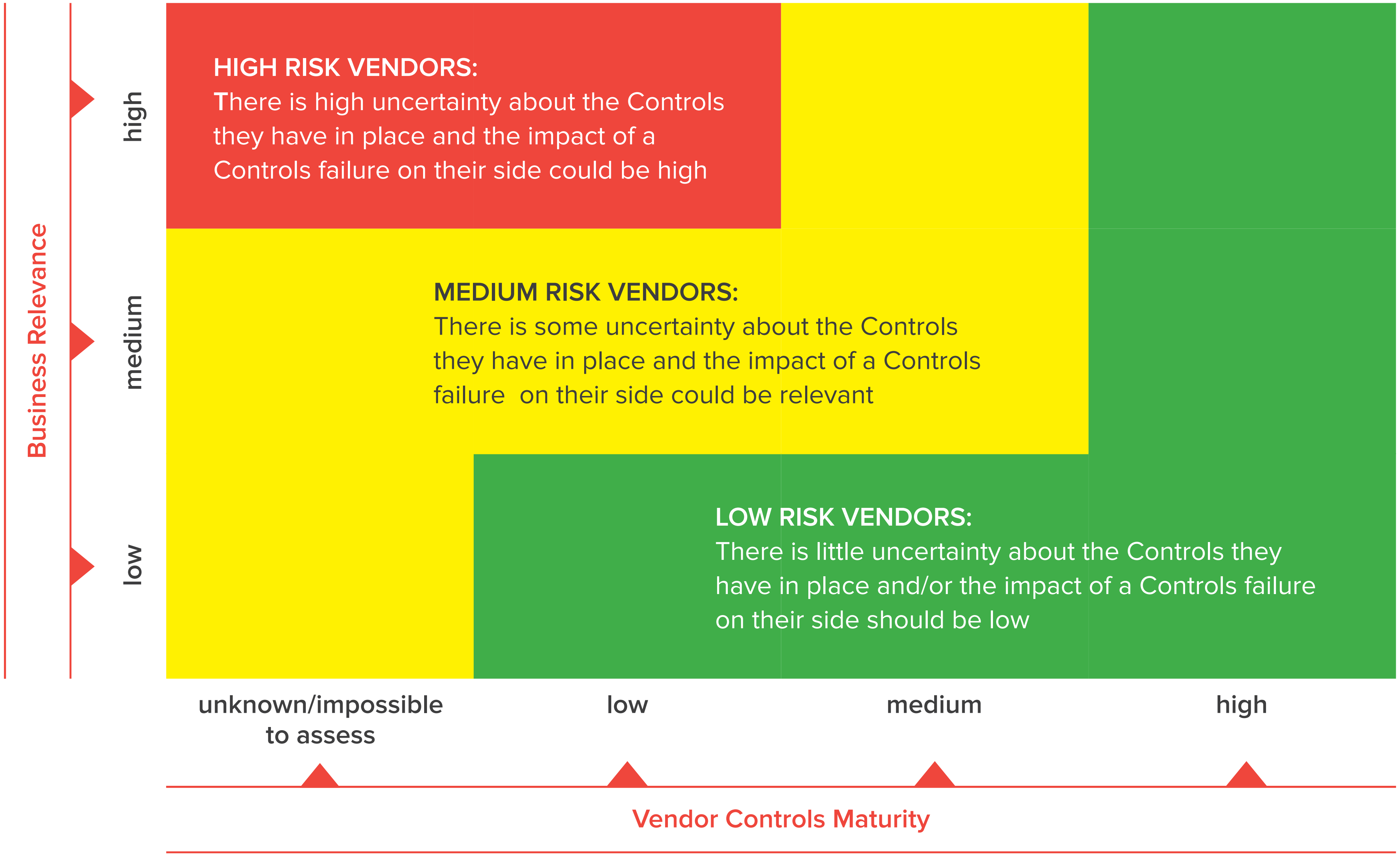


- **Don’t forget to ask about sub-contracting;**
  - – Sometimes a Vendor is only one element in a complex chain of liabilities.
- **Validate the approach with each relationship owner THEN send the short questionnaire to the Vendors;**
  - – You may have to proceed in phases in the event too many relationship owners want to delay the process.
- **Give a realistic but strict deadline (e.g. 2 weeks with a deadline for written questions half way);**
  - – 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 be marked down.

The Risk interpretation


5. Build a detailed programme of work for each high Risk vendor

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

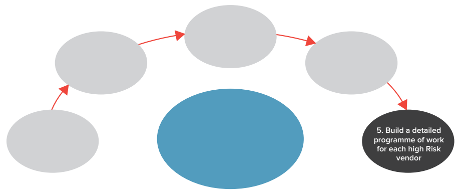


HIGH RISK VENDORS:
There is high uncertainty about the Controls they have in place and the impact of a Controls failure on their side could be high

MEDIUM RISK VENDORS:
There is some uncertainty about the Controls they have in place and the impact of a Controls failure on their side could be relevant

LOW RISK VENDORS:
There is little uncertainty about the Controls they have in place and/or the impact of a Controls failure on their side should be low

5. Build a detailed programme of work for each high/medium Risk Vendor based on the results of the maturity map


5. Build a detailed programme of work for each high Risk vendor

- **You want to focus on high business relevance/low (or unknown) controls maturity Vendors**
- **Detailed programme of work to be validated with each relationship owner and scheduled over a relevant period of time, based on resources available on your side and with the Vendors.**

Multi-days on-site visits and face-to-face meetings with key stakeholders for high risk Vendors;

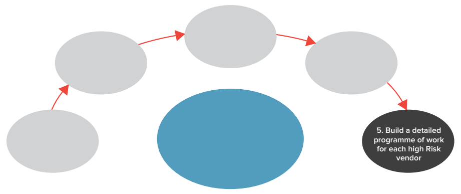
Subject to “right-to-audit” having been obtained contractually or mutual agreement with the Vendor.

Detailed questionaire and Q&A meeting for medium risk Vendors.

In all cases, avoid conflicts and seek a compromise with the Vendor on the rightsizing of the exercise.

Report Vendors who provide insufficient cooperation in line with the Governance Framework established up front.

5. Build a detailed programme of work for each high/medium Risk Vendor based on the results of the maturity map


5. Build a detailed programme of work for each high Risk vendor

- **Both approaches to be run against a broader set of controls taken out of existing internal policies and/or industry good/best practices**
  - – With the view of determining key areas of controls deficiencies and agreeing a remedial plan of action with the vendor.

- **Progress against agreed remedial plan of action to be tracked in accordance with a schedule agreed with each Vendor.**

- **Consider following up legally (e.g. asking your legal team to communicate findings and agreed actions formally) where business & management believe it is appropriate**
  - – In relation to the business relevance of the vendor, the state of the relationship, the lack of cooperation or the lack of progress.

Contact

For further information please contact:

Jean-Christophe Gaillard
Managing Director
+44 (0)7733 001 530
jcgaillard@corixpartners.com

Neil Cordell
Director
+44 (0)7701 015 275
neilcordell@corixpartners.com

www.corixpartners.com