A balanced approach to Cloud computing

How to articulate a Risk analysis for Cloud services

corix partners

The “Cloud”: Nothing particularly new…

Evolution, not revolution

– The IT industry has a long established tradition of re-inventing itself; this is just another cycle; it comes with considerable marketing and hype

– The expression “The Cloud” in itself is misleading : Not a single concept, but a range of diverse services packaged in different ways: SaaS, PaaS, IaaS, etc … / Public / Hybrid / Private

– Those have been evolving and consolidating for the last 5-10 years; they are not new in any way by themselves

Bottom line: It’s the same old IT

– Datacentres (they burn!) / Networks (they break!) / Hardware (it fails!) / Software (never works!) / People (they make mistakes!)

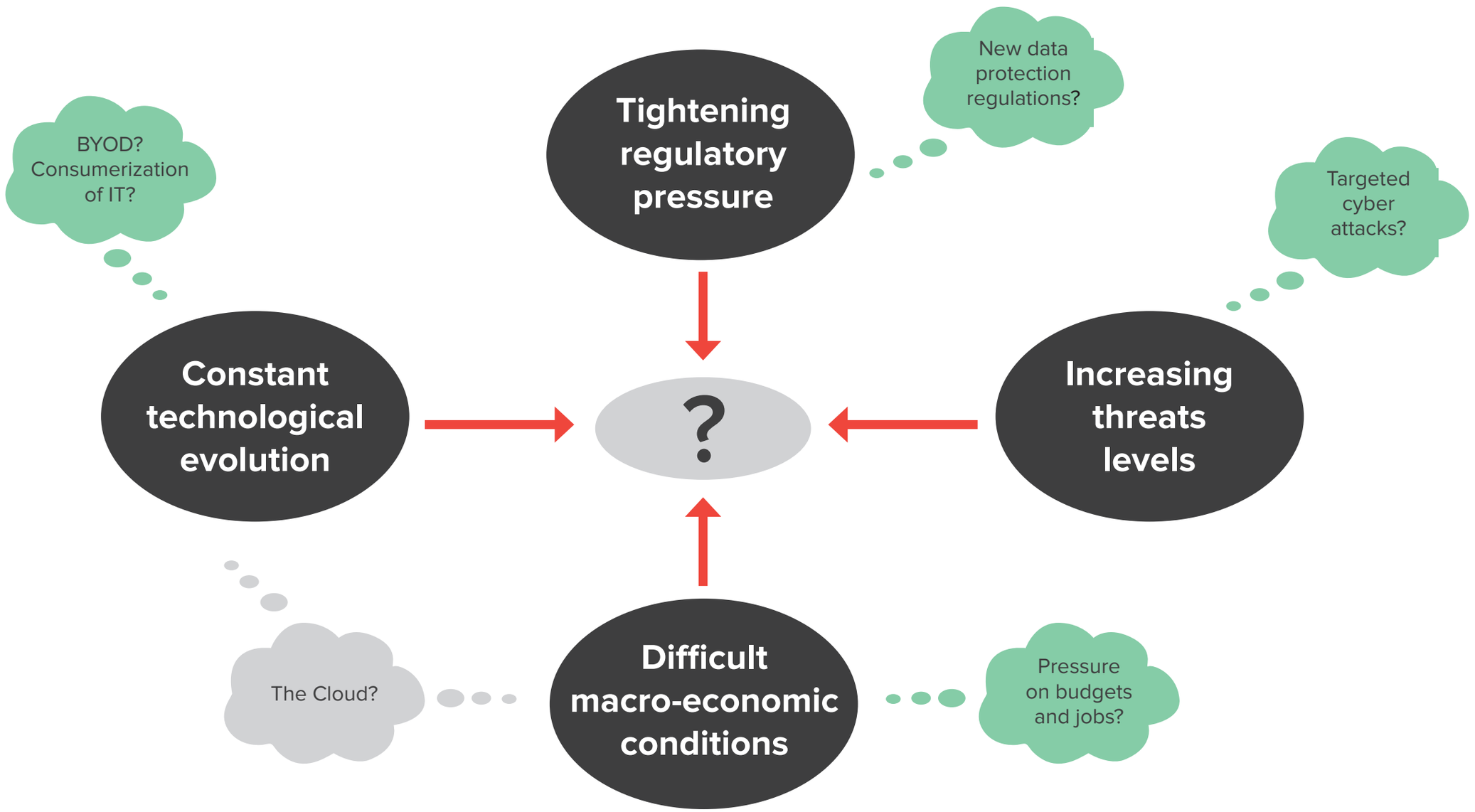
– Don’t be naïve (there is no “Cloud”) and let your own experience guide you

IT commoditization can bring real advantages in terms of operational & financial efficiency, but please cut through the hype!

CIOs should put all aspects into perspective and base Cloud decisions (like most others) on a balanced risk and rewards analysis

Why?

- **Because the Cloud is only one aspect in a bigger picture: Today's CIO challenge is to deliver robust, cost-efficient, business-aligned IT services, in a context of:**



Security in the Cloud: Should you be concerned?

- **YES and NO**
  - The Cloud presents a number of specific attributes that bring new Security challenges
  - But standard good practices for Security, outsourcing and Risk management (if in place) will go a long way to protecting you and your information in the Cloud
- **Do not not separate "Security in the Cloud" from your ongoing practice of IT and Information Security, and your own current maturity (good or bad) in that space**

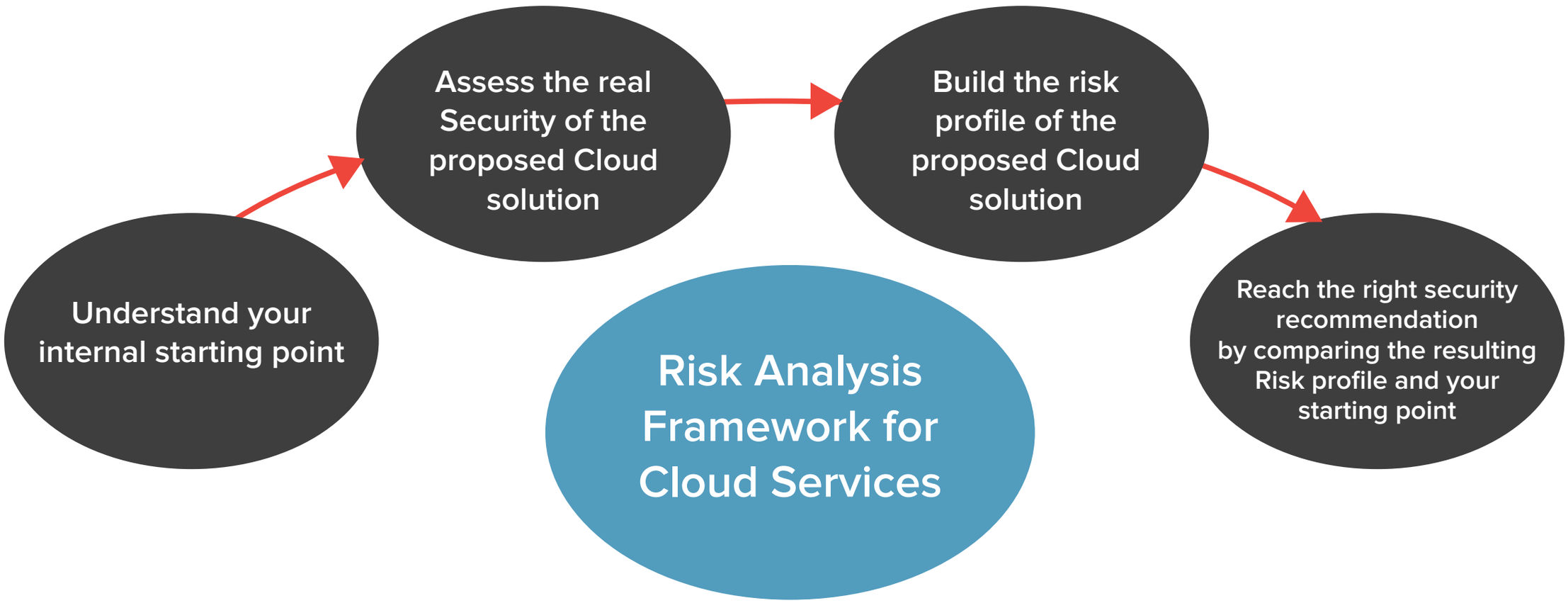
There is no short-cut or magic technical trick

Approach "Security in the Cloud" with an open mind

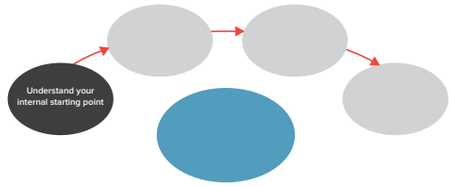
Do not take it for granted (either way)

Establish the basis on which informed Security descisions can be made, taking into account all relevant aspects

The real Cloud Security challenge:



The real Cloud Security challenge.



Buliding up the Security Risk profile of the proposed Cloud solution

START INTERNALLY

Step 1 → **Establish a level playing field:**

Understand what is on the table; remove language issues and the marketing buzz; assemble all internal stakeholders; separate private cloud issues from hybrid / public Cloud issues

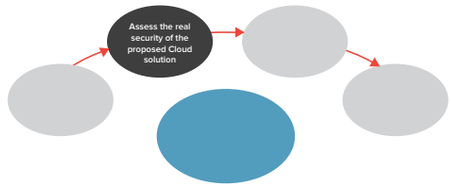
Step 2 → **Assess the sensitivity of the information being pushed into the Cloud:**

Financial / Reputational / Legal / Regulatory sensitivity

Step 3 → **Understand the way the information being pushed into the Cloud needs to be protected AND the way it is actually protected internally to start with:**

What is your internal policy framework on the matter? Is there one? Who owns it? How is it currently applied? i.e. how is information currently protected in-house?

The real Cloud Security challenge



THEN

Step 4 → **Assess the real processing chain that your information will follow while in the Cloud:**

Number of players involved; nature of the interaction / partnership between them

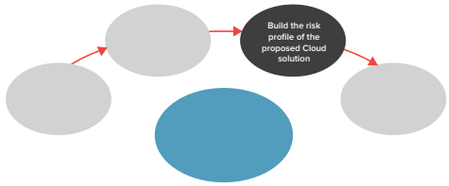
Step 5 → **Examine in detail Legal & Services terms for the proposed Cloud service:**

In light of the sensitivity of the information being pushed into the Cloud; in light of the chain of processing

Step 6 → **Assess the Security capability & maturity of all relevant players along the processing chain:**

Through a number of due-diligence assessments

The Security Risk profile



Step 7 → **Assemble**

results into a high level Risk profile for the proposed Cloud solution

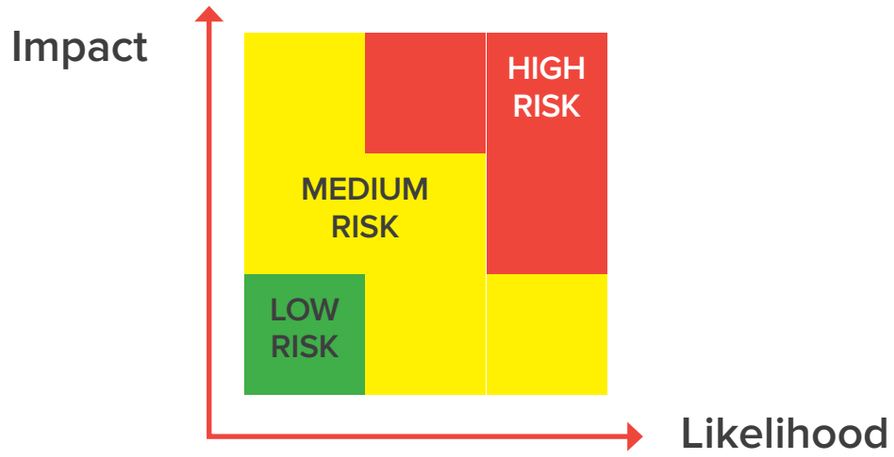
What drives the IMPACT Analysis?

1 – Business (Financial & Reputational) / Regulatory / Legal Information Sensitivity

2 – Analysis of ALL service contracts and legal terms with the Cloud Service Provider(s), and the mitigating elements they may offer (or not)

- Do they guarantee that your information will be handled and protected the way it should be (in relation to its sensitivity)?

3 – Analysis of insurance schemes that may exist to migrate financial impact (where applicable)



What drives the LIKELIHOOD Analysis?

1 – Full understanding of the real chain of information processing in the Cloud

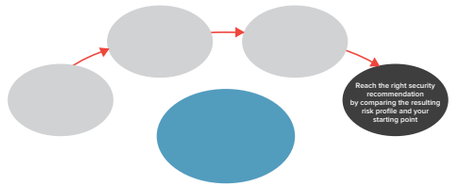
- How transparent is it ?

2 – Assessment of the Security capability & maturity of ALL thirdparties involved in the Cloud processing chain

- Can they protect your information the way it should be (in relation to its sensitivity) ?

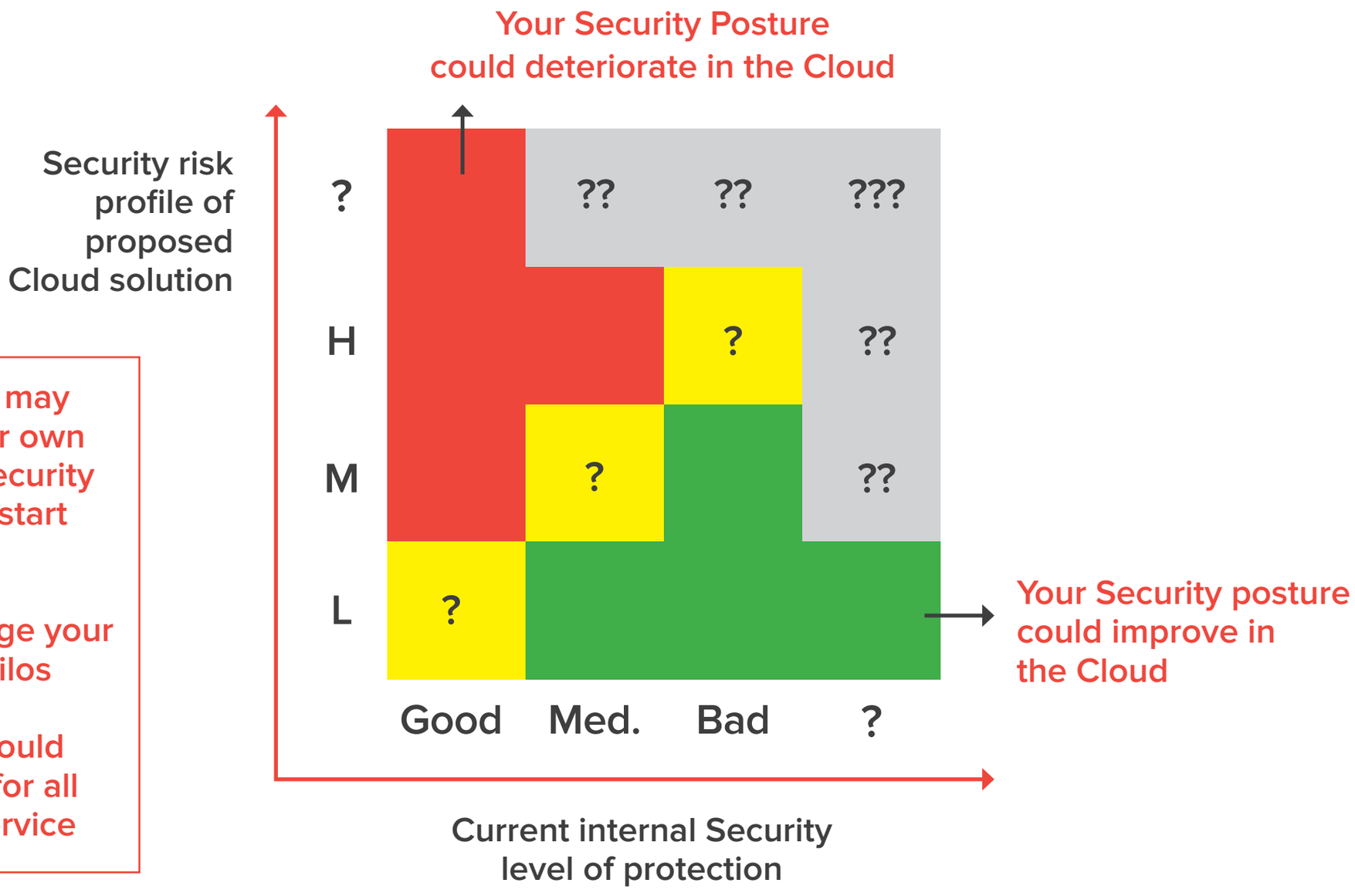
- Can they react to abnormal situations ?

The Security recommendation



Step 8 → **Finally, compare**

the Security Risk profile of your proposed Cloud solution to your Security starting point (if applicable)



The approach may challenge your own Information Security maturity from start to end

It may challenge your own internal silos

In fact, you should be doing this for all outsourced service

Step by step: Key do's and don'ts

Do

- Take information sensitivity as your main guide and stick to it; sensitive information must be protected (in the Cloud or not)
- Take the legal aspects seriously ; they are often one-sided and only favourable to the service provider but they are an integral part of what the Cloud really is
- Make sure the legal review is driven by a person directly familiar with the service being pushed into the Cloud
- Push back on ludicrous terms
- Build on your own experience and aim at forming a structured opinion about the provider's security posture
- Keep third-party Security assessments as simple as possible; a 10 points checklist and site visit can go a long way; involve yourself to form your own opinion

Do Not

- Allow (perceived or alleged) contract value to rule alone
- Treat the legal aspects as a legal exercise to be offloaded to some legal expert
- Attempt an exhaustive enumeration of specific risk scenarios
- Treat third-party Security assessments as a pure paper exercise

Step by step: Key do's and don'ts

Do

- Make sure you talk to the right Security people i.e. the people who would be directly involved with the Security of the service you are considering
- Look behind the curtains and ask questions; value transparency and honesty
- Value certifications but understand what they are worth; they can hide a variety of practices and they are not a silver bullet
- Treat the unknown as unknown and factor it in your Risk analysis; what you don't know can be as important as what you do know
- Price Risk and incidents into your cost models, in particular for large scale projects, and if you end-up with an unfavourable Risk profile

Do Not

- Accept Security brochureware
- Rely only on SAS70 assessment and the like; they can be manipulated or misleading
- Assume the Cloud is right / cheap for you because it is right /cheap for others
- Sign contracts until you can properly balance risk & rewards, in view of the full picture

The specifics of the Cloud

1 Commoditization

- **This type of Risk examination deconstructs the Cloud and goes against its fabric:**
  Cloud services are mostly sold as cheap and transparent
- **You may not get the level of flexibility you need on Legal & Service terms, or the level of transparency you want regarding Security practices:**
  compared to more conventional outsourcing arrangements
- **The backdoor is already wide open:**
  Many commoditized services are being sold directly into your business; you may not catch any of this before it's too late

2 Marketing and Hype

- **You may find lower than expected Security maturity levels:**
  with quite a few vendors having jumped late on the Cloud bandwagon without a full appreciation of your Security requirements & expectations

Both specifics will tend to push Risk Profiles up

Keep assessments as simple as you can, put a time limit on your Risk analysis exercise and factor the residual unknown into your results

Consider pricing Risk and incidents into costs model if you end up having to accept an unsatisfactory Risk profile

Conclusion

- **You can be more secure in the Cloud:**
  Your own initial security maturity (or the lack of it) is a parameter, as well as the Security capability and maturity of Cloud service providers and other aspects

- **Do not trust blindly**
  Even if the Security Risk analysis is complex and challenges your own security maturity and your own internal silos

- **Challenge service providers**
  Even if it goes against the fabric of the Cloud; in a structured manner until you are satisfied you have enough information (positively or negatively) to drive an informed decision regarding Security matters

- **Factor all associated costs**
  Into costs models and projects as early as possible, including Risk and incidents if applicable

- **Do not treat the Risk analysis exercise as a one-off**
  But manage the relationship on an ongoing basis and revisit the Risk analysis periodically

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