RSAConference2018
San Francisco | April 16–20 | Moscone Center

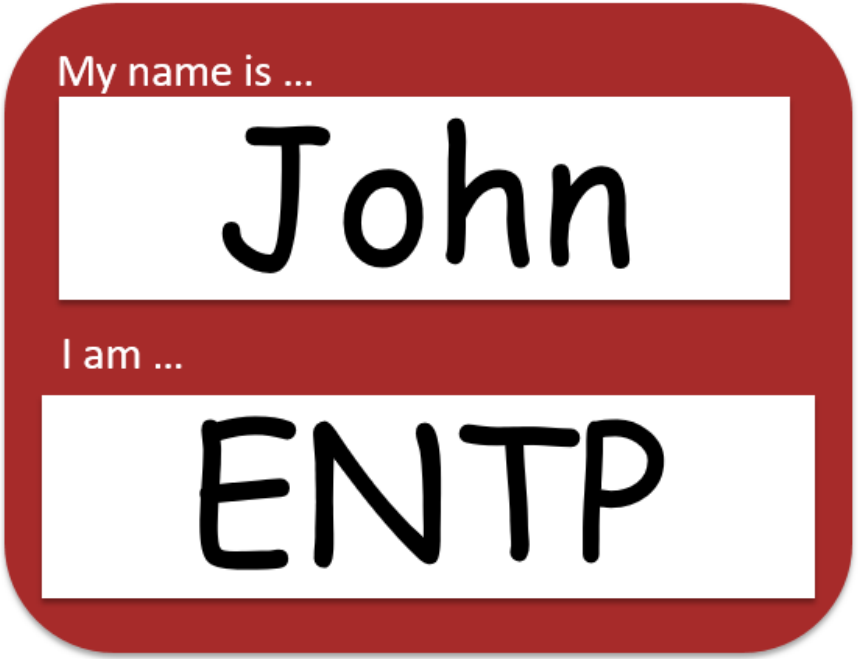
SESSION ID: STR-T08

PERSONALITY PROFILING YOUR THIRD PARTIES FOR EFFECTIVE SUPPLIER MANAGEMENT

John Elliott

Data Protection Officer @ Large European Airline | Author @ Pluralsight
@withoufire

Hello



ENTP

- **E – Extroversion preferred to introversion:** ENTPs gain energy through interactions with people or objects in the outside world.
- **N – Intuition preferred to sensing**: ENTPs tend to be more abstract than concrete. They focus their attention on the big picture rather than the details first, and on future possibilities rather than immediate realities.
- **T – Thinking preferred to feeling:** ENTPs tend to value objective criteria above personal preference. When making decisions, they generally give more weight to logic than to social considerations.
- **P – Perception preferred to judgment**: ENTPs tend to withhold judgment and delay important decisions, preferring to "keep their options open" should circumstances change.

I should be good at …

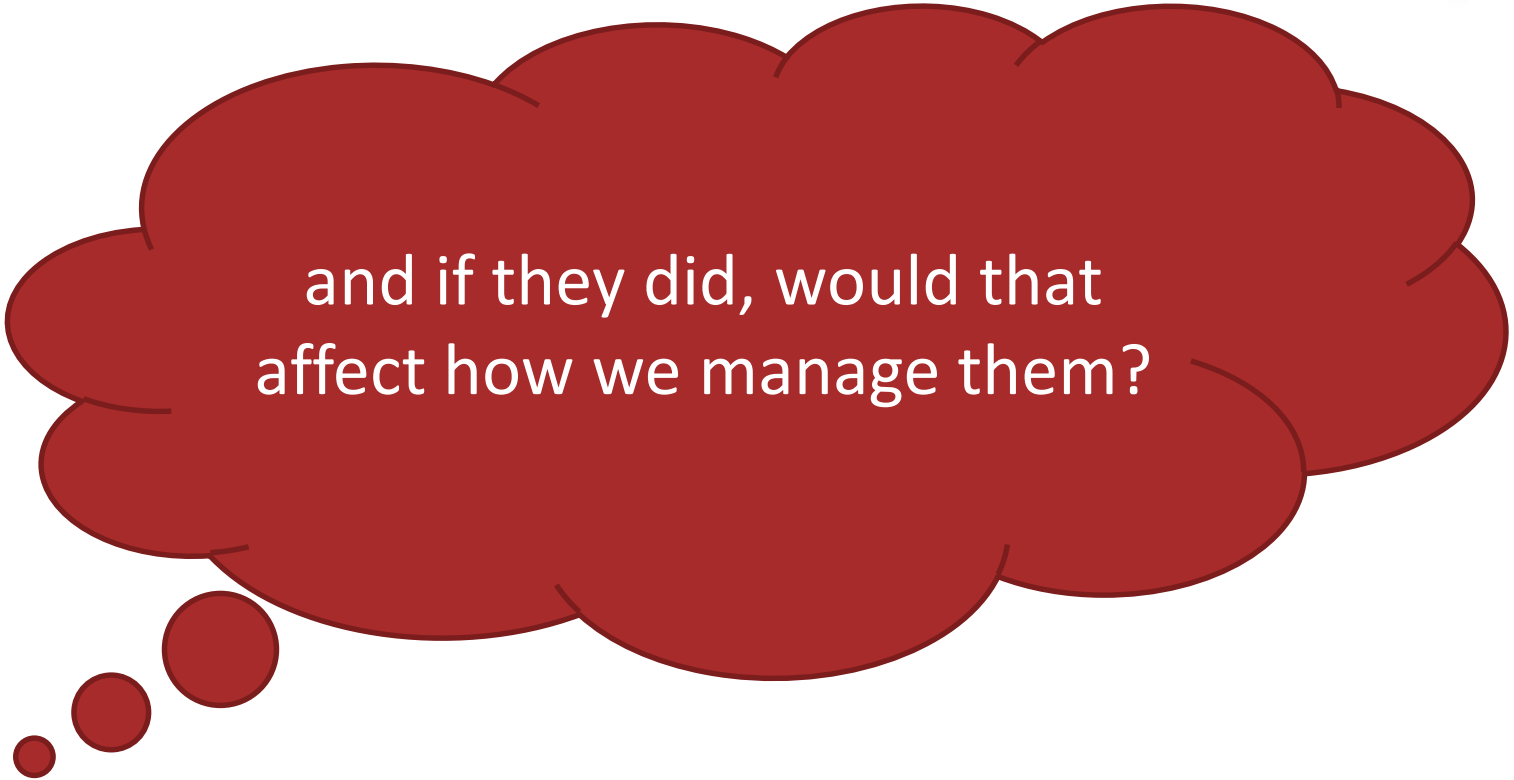
- Innovation
- Original thoughts
- Invention
- Visionary things
- Being a Lawyer (!)

I’m not awesome at …

- Following through with detailed plans
- Thinking of the needs of other people
- Single tasking
- Responding well to authority….

Here's my thought

Here's my thought



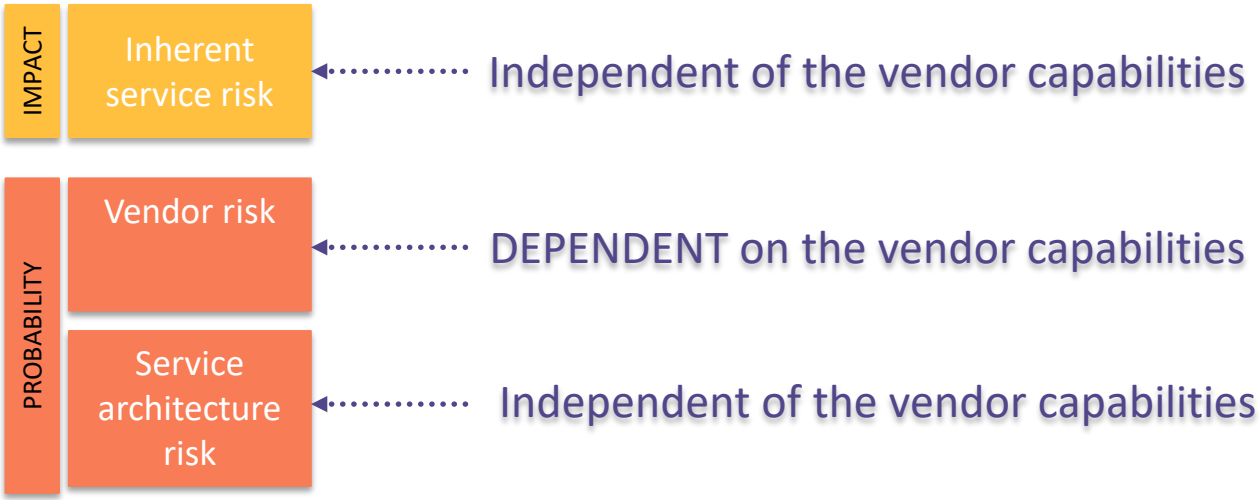
Starting Point

This has nothing to do with compliance

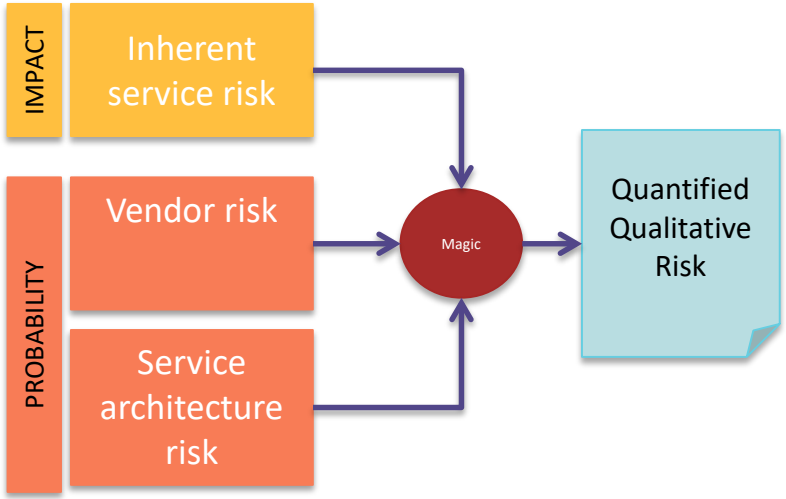
Which third parties are most likely to lose data

What can I do to minimize this risk

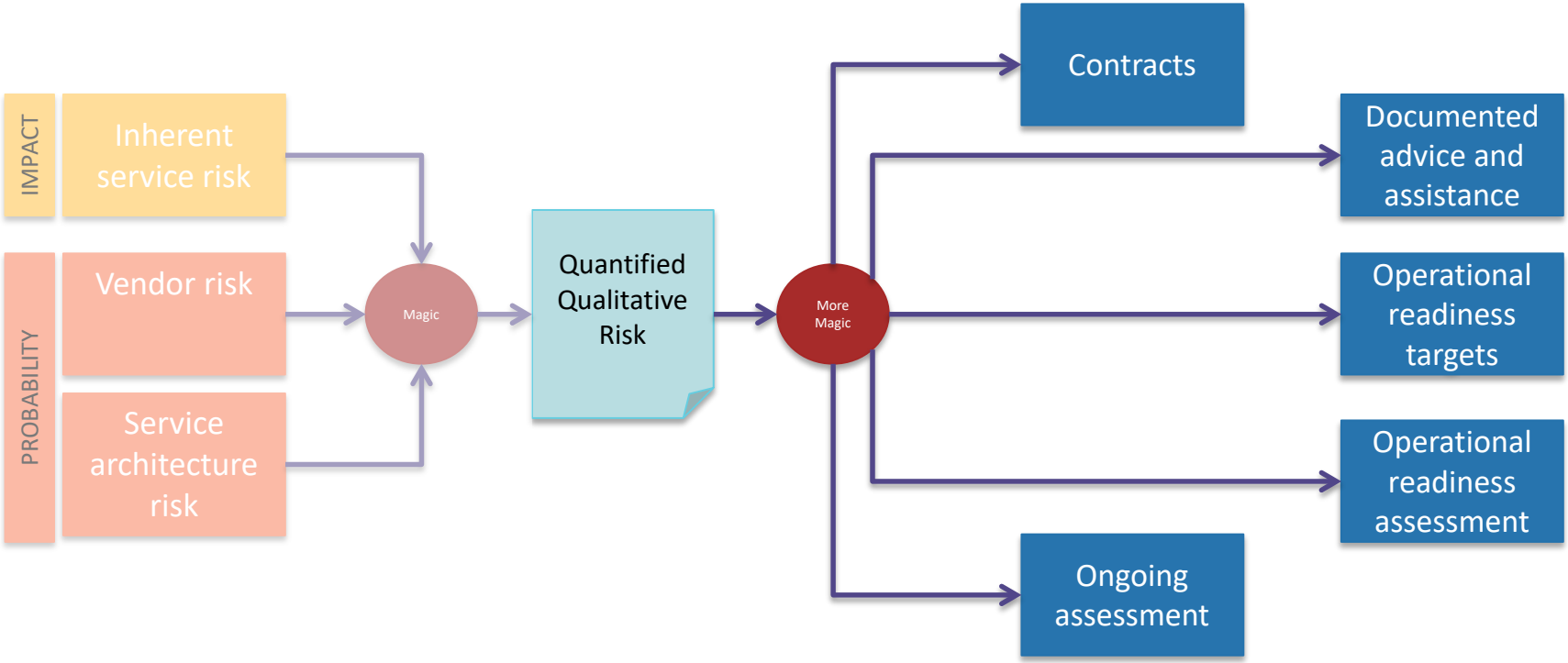
Vendor / Supplier / 3rd Party risk is …



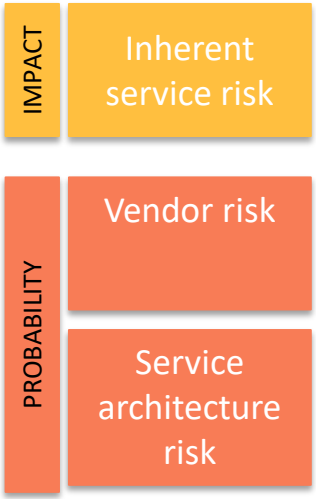
Vendor risk is …



Vendor risk is …

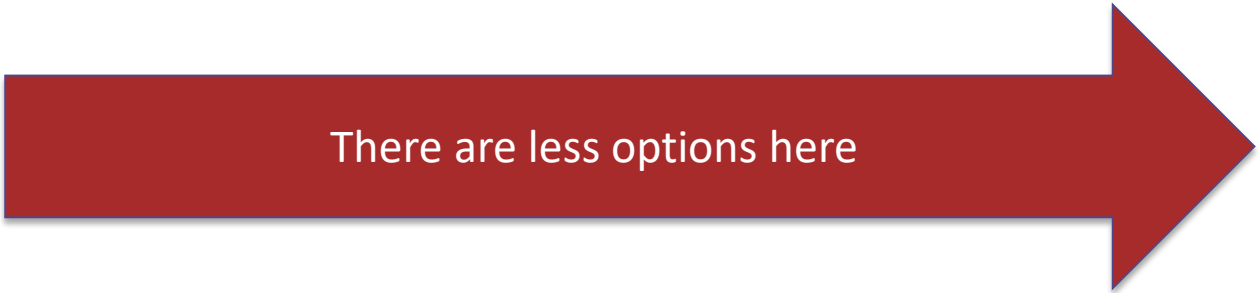


Vendor risk is …



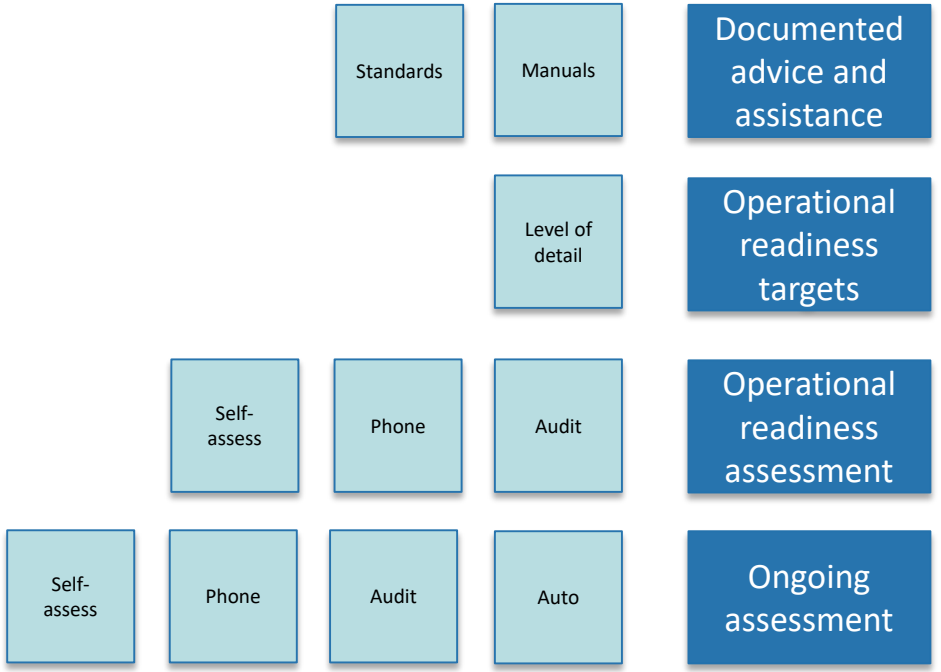
There could be infinite variables here

Vendor risk is …

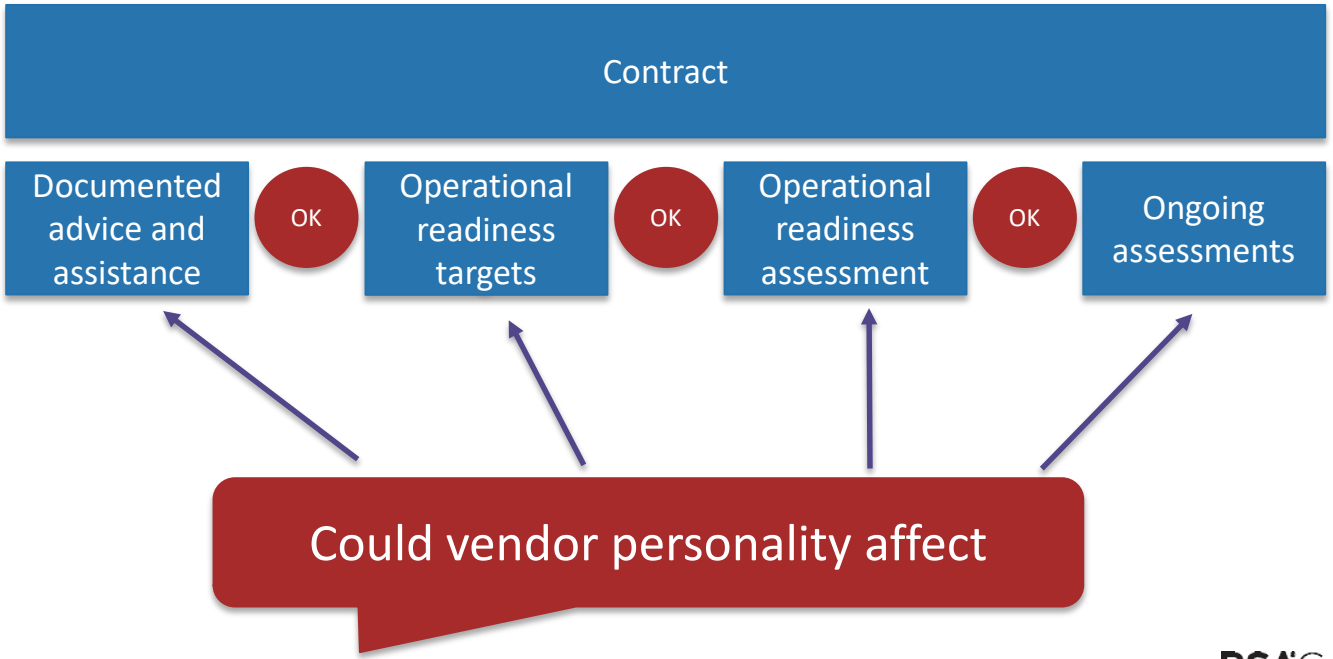


- Documented advice and assistance
- Operational readiness targets
- Operational readiness assessment
- Ongoing assessment

Vendor risk is …



Process


Contract
Documented advice and assistance
OK
Operational readiness targets
OK
Operational readiness assessment
OK
Ongoing assessments
Could vendor personality affect

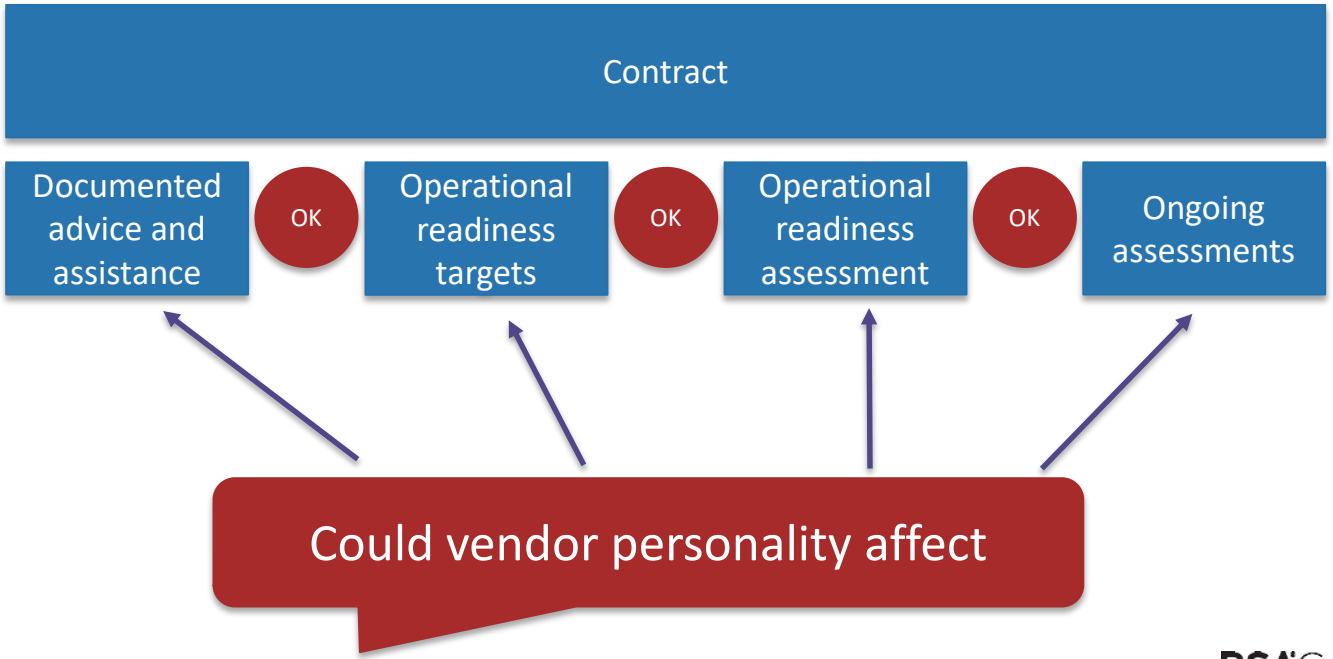
3-axis of supplier personalities

Knowledge	Ignorant	Know
Able to execute	Unable	Able
Intent to execute	Negative	Positive

Vendor Personality Types

Knowledge	Ability	Intent		
Know	Able	Positive	KAP:	Dream supplier
Know	Able	Negative	KAN:	Deceivers
Know	Unable	Positive	KUP:	Frustrators
Know	Unable	Negative	KUN:	Theorists
Ignorant	Able	Positive	IAP:	Dunning Krugers
Ignorant	Able	Negative	IAN:	Bureaucrats
Ignorant	Unable	Positive	IUP:	Puppies
Ignorant	Unable	Negative	IUN:	Freddie Krugers

Process



Process

Knowledge	Contract: Documented advice and assistance	Contract: Operational readiness targets	Contract: Operational readiness assessment	Contract: Ongoing assessments
Know		high-level	self	phone
Ignorant	Extensive+ follow up	detailed	onsite	onsite

Process

	Contract			
Able to execute	Documented advice and assistance	Operational readiness targets	Operational readiness assessment	Ongoing assessments
Able			self	self
Unable		detailed	onsite	phone

Process

Intent to execute	Contract: Documented advice and assistance	Contract: Operational readiness targets	Contract: Operational readiness assessment	Contract: Ongoing assessments
Positive			self	self
Negative		detailed	onsite	continuous

Vendor Personality Types

Know	Able	Intend
Know	Able	Positive
Know	Able	Negative
Know	Unable	Positive
Know	Unable	Negative

Docs & assist	OR Targets	OR Assess	Ongoing
		Self	Self
	Detailed	Onsite	Onsite
		Onsite	Phone
	Detailed	Onsite	Continuous

Vendor Personality Types

Know	Able	Intend
Know	Able	Positive
Know	Able	Negative
Know	Unable	Positive
Know	Unable	Negative
Ignorant	Able	Positive
Ignorant	Able	Negative
Ignorant	Unable	Positive
Ignorant	Unable	Negative

Docs & assist	OR Targets	OR Assess	Ongoing
		Self	Self
	Detailed	Onsite	Onsite
		Onsite	Phone
	Detailed	Onsite	Continuous
Extensive+ follow up	Detailed	Phone	Self
		Onsite	Onsite
		Onsite	Phone
		Onsite	Continuous

Vendor Personality Types

#RSAC

Know	Able	Intend
Know	Able	Positive
Know	Able	Negative
Know	Unable	Positive
Know	Unable	Negative
Ignorant	Able	Positive
Ignorant	Able	Negative
Ignorant	Unable	Positive
Ignorant	Unable	Negative

Docs & assist	OR Targets	OR Assess	Ongoing
		Self	Self
	Detailed	Onsite	Onsite
		Onsite	Phone
	Detailed	Onsite	Continuous
Extensive+ follow up	Detailed	Phone	Self
		Onsite	Onsite
		Onsite	Phone
		Onsite	Continuous

Vendor Personality Types

Know	Able	Intend	Docs & assist	OR Targets	OR Assess	Ongoing
Know	Able	Positive			Self	Self
Know	Able	Negative		Detailed	Onsite	Onsite
Know	Unable	Positive			Onsite	Phone
Know	Unable	Negative		Detailed	Onsite	Continuous
Ignorant	Able	Positive	Extensive+ follow up	Detailed	Phone	Self
Ignorant	Able	Negative			Onsite	Onsite
Ignorant	Unable	Positive			Onsite	Phone
Ignorant	Unable	Negative			Onsite	Continuous

Remember, this is just a model

SO HOW CAN YOU ASSESS A VENDOR'S PERSONALITY?

Sniff test

External Ratings (also sniff test)

SecurityScorecard

BITSIGHT®
The Standard in SECURITY RATINGS

UpGuard™

But beware of …

Know	Able	Negative

Ask Open Questions

Make the vendor think

Demonstrate knowledge, ability or intent

Force deceitful declarations

Can not be completed by sales

Ask open questions

Q. What do you see as the top three cyber threats to your business?

Ask open questions

Q. How do you gain short-,medium- and long-term threat intelligence?

Ask open questions

Q. What formal and informal information sharing networks are you members of?

Ask open questions

Q. How many days of professional resource have been used in penetration testing and ‘red team’ tests or other similar assurance exercises in the past twelve months?

Ask open questions

…What do you plan to do differently next year?

Ask open questions

Q. How many people have more than 50% of their role allocated to cyber/information security responsibilities?

Ask open questions

…Do you think this is enough?

Ask open questions

Q. How many person-days have you estimated would it take a malicious external attacker to breach your defenses and gain privileged access to critical systems?

Ask open questions

…How quickly would you detect this type of intrusion into your network?

Ask open questions

…How many intrusions have you detected in the past twelve months?

Ask open questions

Q. What are the RPO, RQO and RTO for the systems that support the service you provide to us?

Ask open questions

… When you last did a test what RTO, RPO and RQO did you achieve?

Ask open questions

Q. Have you formally appointed a Data Protection Officer (DPO)?
If so, who is this.

Ask open questions

… If so, who is this …

Ask open questions

… and what are their qualifications …

Ask open questions

Q. What processes do you have in place to respond to Data Subjects who request their data in accordance with GDPR Article 15?

Ask open questions

Q. How will you detect a ‘Personal Data Breach’?

What's interesting?

Non-answers

We have ISO27001 and our CISO is awesome answers

Long answers

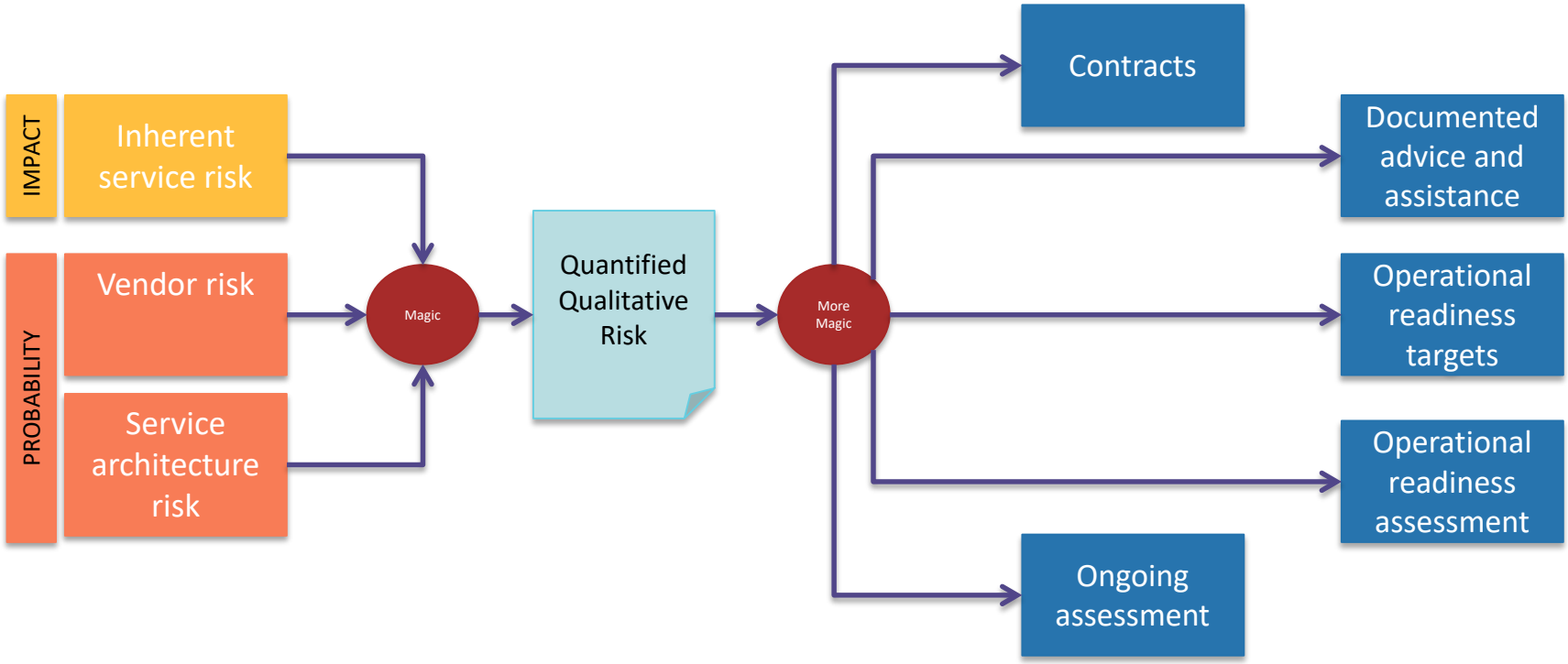
What's interesting?

This is far too confidential

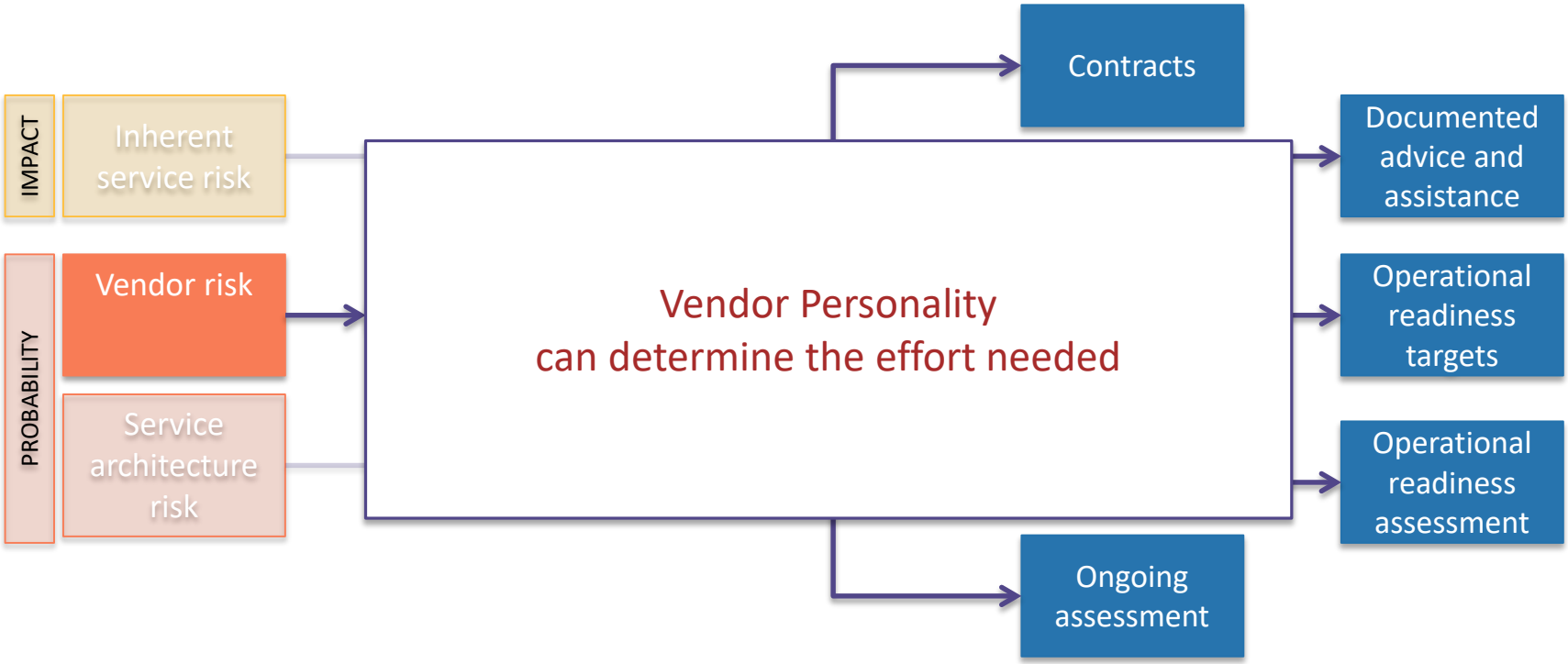
Everything is outsourced to XXX

No one asked us this before

Summary …


IMPACT
Inherent service risk
PROBABILITY
Vendor risk
Service architecture risk
Magic
Quantified Qualitative Risk
More Magic
Contracts
Documented advice and assistance
Operational readiness targets
Operational readiness assessment
Ongoing assessment

Summary …


IMPACT
Inherent service risk
PROBABILITY
Vendor risk
Service architecture risk
Vendor Personality
can determine the effort needed
Contracts
Ongoing assessment
Documented advice and assistance
Operational readiness targets
Operational readiness assessment

Taking this back to the office

- Isolate the levers (approaches) you use to gain supplier assurance
  - Do you use operational readiness targets
- Can you save resources by profiling suppliers?
  - This exercise is not free
- Would it save compliance-related activities?
- Try a sample questionnaire on some suppliers

QUESTIONS

Or @withoutfire