

Presented by:  
Christopher S. Ellingwood, CISA



VENDOR DUE DILIGENCE  
PROACTIVE APPROACHES TO BETTER  
UNDERSTAND YOUR VENDORS

# CHRISTOPHER S. ELLINGWOOD, CISA

IT Assurance Manager  
BerryDunn  
Management and  
Information Technology  
Consulting Group



# AGENDA

- Why is vendor due diligence important?
- What vendors do I include?
- It's all about the risk
- A little more than collecting documents
- A note on SOC (SSAE 16) exams

WHAT IS VENDOR DUE  
DILIGENCE?

WHY DO WE CARE?







**YOUR VENDORS  
ARE FINANCIALLY  
MATERIAL TO YOUR  
BUSINESS**

# DEVELOPING A VENDOR DUE DILIGENCE PROGRAM

Risk

Enter

# STEP 1: IDENTIFY AND CLASSIFY






## STEP 2: IDENTIFY THE POSSIBLE RISK










**To Consider:** The Risk that your outsourced data center loses power and your systems are unavailable

Risk:	Likelihood to occur	Impact of risk			Overall risk rating
		Financial	Security	Operational	
 <b>High</b>	Low likelihood: 1	Low impact: 1	Low impact: 1	Low impact: 1	Low overall risk: 4 - 5
 <b>Medium</b>	Medium likelihood: 2	Medium Impact: 2	Medium Impact: 2	Medium Impact: 2	Medium overall risk: 6 - 8
 <b>Low</b>	High Likelihood: 3	High Impact: 3	High Impact: 3	High Impact: 3	High overall risk: 9 - 12

**GAIN CONTROL**

# FOR EXAMPLE....

Risk:	Likelihood to occur	Impact of risk			Overall risk rating
The risk that our outsourced data center loses power and our systems are unavailable		Financial	Security	Operational	
	 Low 1	 Medium 2	 Low 1	 High 3	 Medium 7

GAIN CONTROL



**DON'T FORGET COMPLIANCE  
AND REGULATIONS**

An hourglass with red sand is shown against a dark background. The sand is flowing from the top bulb to the bottom bulb, creating a thin stream in the middle. The top bulb is partially filled with red sand, and the bottom bulb is also partially filled. The hourglass is centered on the left side of the image.

**STEP 3:  
DEVELOP A  
SCHEDULE**

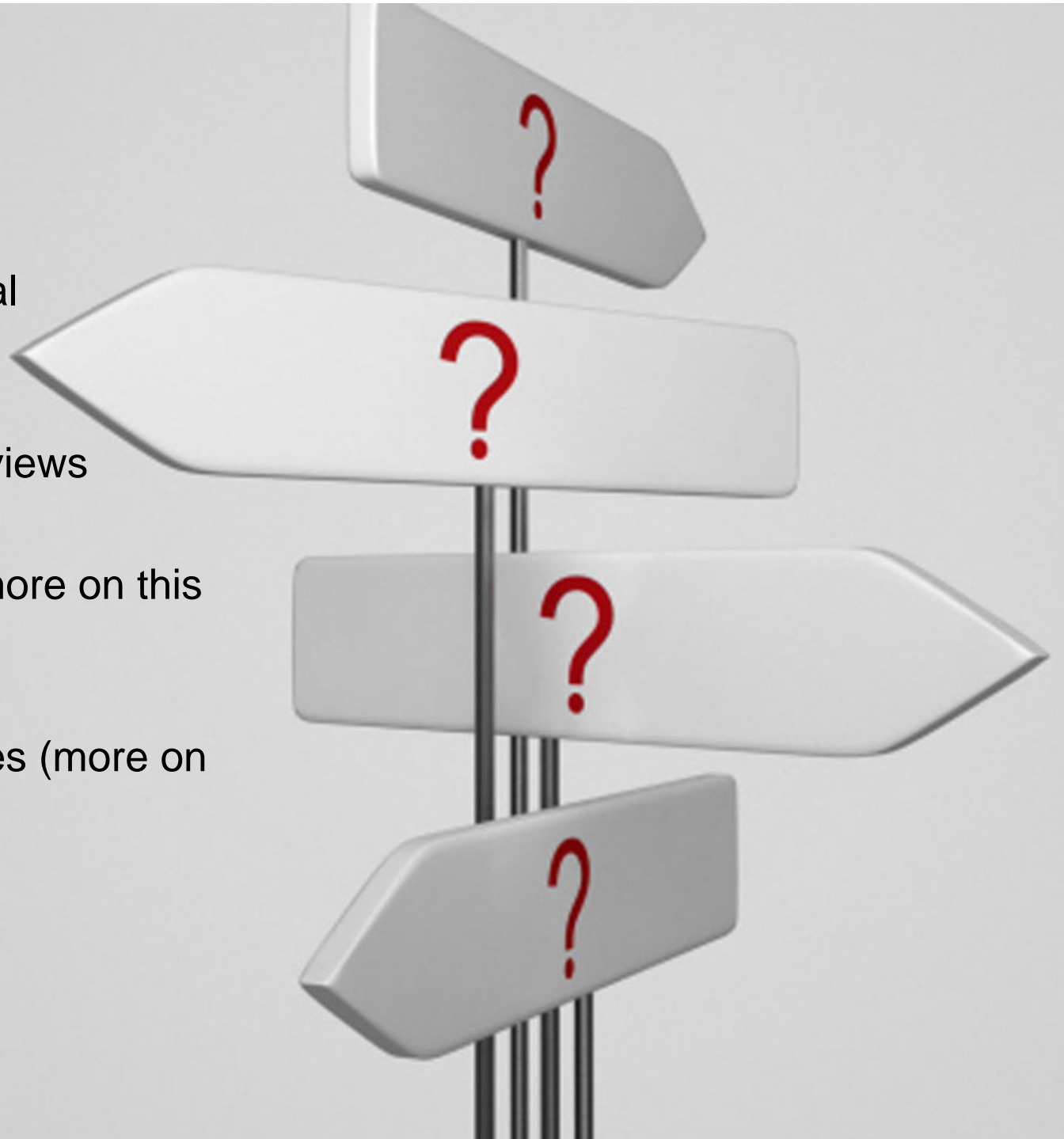


WHAT DO I ASK FOR?



## REQUESTS -

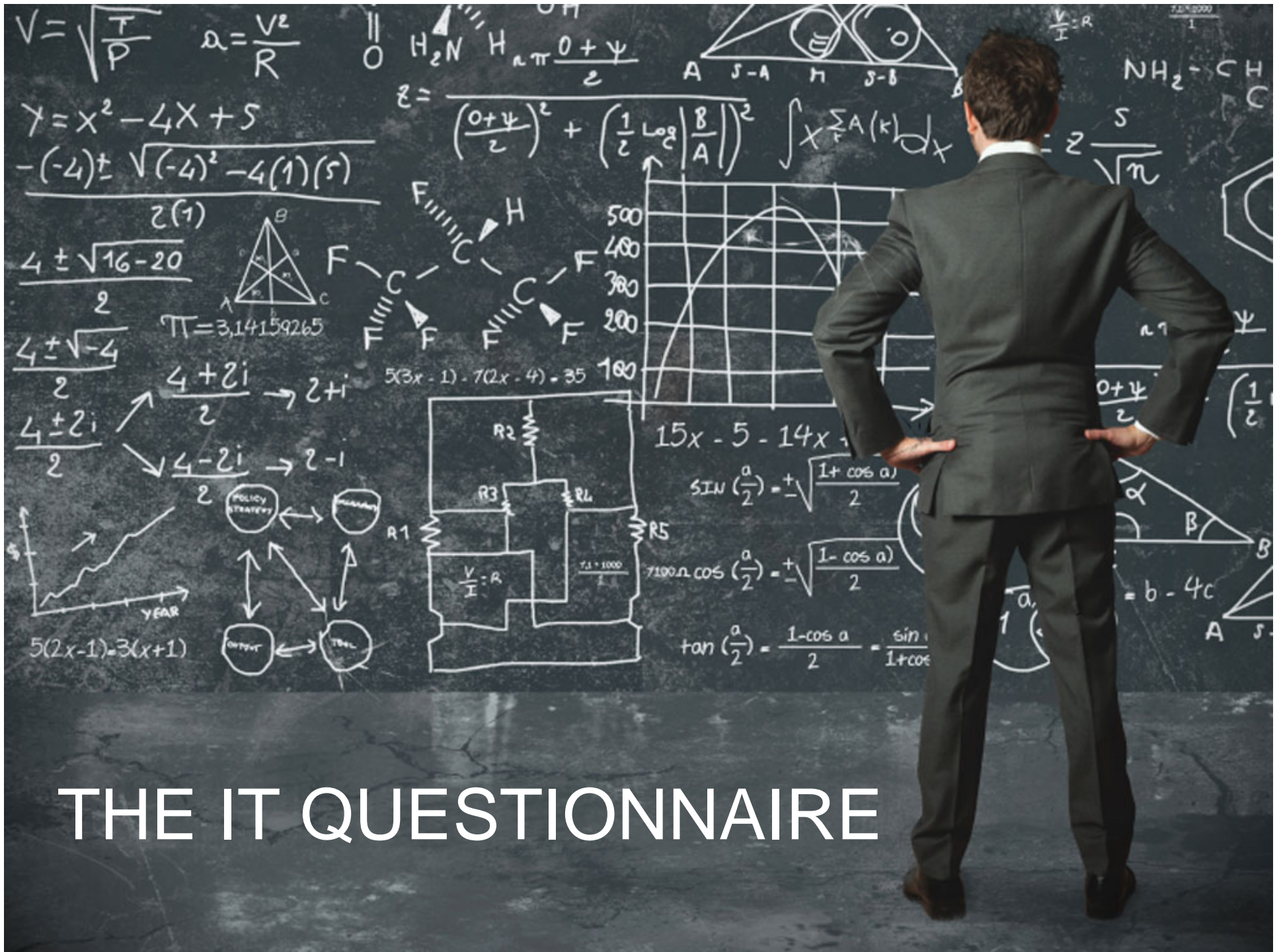
- Audited Financial Statements
- Compliance Reviews
- SOC Reports (more on this shortly)
- IT Questionnaires (more on this as well)



# THE EVER-IMPORTANT SOC REPORT







# THE IT QUESTIONNAIRE



A photograph showing a stack of seven books on the left, with a silver laptop on the right. The books have various colored covers: blue, white, blue, red, blue, blue, and purple. The laptop is open, and its screen is tilted upwards. The text "DOCUMENT YOUR REVIEW" is written in red, bold, sans-serif font in the upper right quadrant of the image.

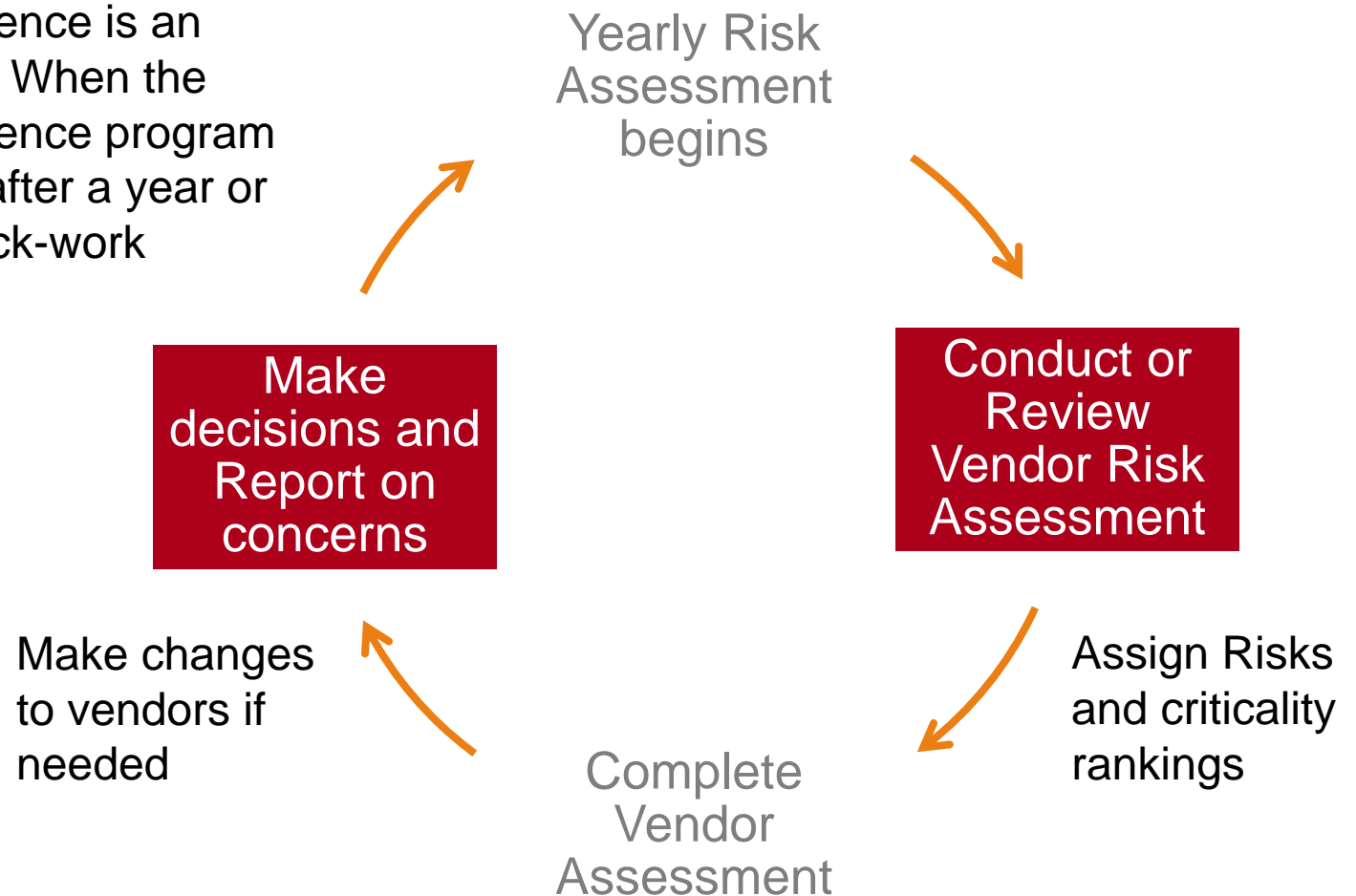
# DOCUMENT YOUR REVIEW

**REPORT YOUR FINDINGS**



# THE PROCESS (SUMMARY)

Vendor Due Diligence is an ongoing process. When the Vendor Due Diligence program is implemented, after a year or so it runs like clock-work





A SUCCESSFUL  
PROGRAM  
WILL...



QUESTIONS?



# INTERESTED IN MORE?

We are always available for your questions



[cellingwood@berrydunn.com](mailto:cellingwood@berrydunn.com)