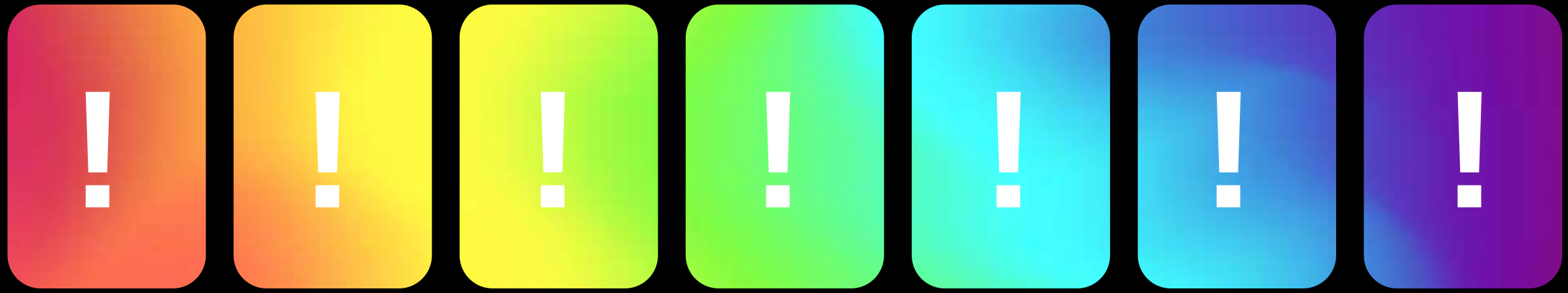


WELCOME

ADAPTIVE GRC

ADAPTIVE GRC

Raiders of the Lost Compliance:

Indiana Jones' approach to Third-Party compliance and risk management

Jan Anisimowicz
Board Member, C&F SA Poland
AdaptiveGRC product

ADAPTIVEGRC

Jan Anisimowicz

Board Member, C&F SA Poland

AdaptiveGRC product

Key facts about C&F, owner of AdaptiveGRC

For over 20 years, C&F has been providing solutions for the largest international organizations, including those from the Fortune 500 list.

Our clients include companies from the following sectors:

- Banking
- Financial Services
- Pharma and life sciences
- Animal health
- Transport/logistics
- Human Resource Management

20+ Over two decades of **experience** in cooperation with the largest companies in the world

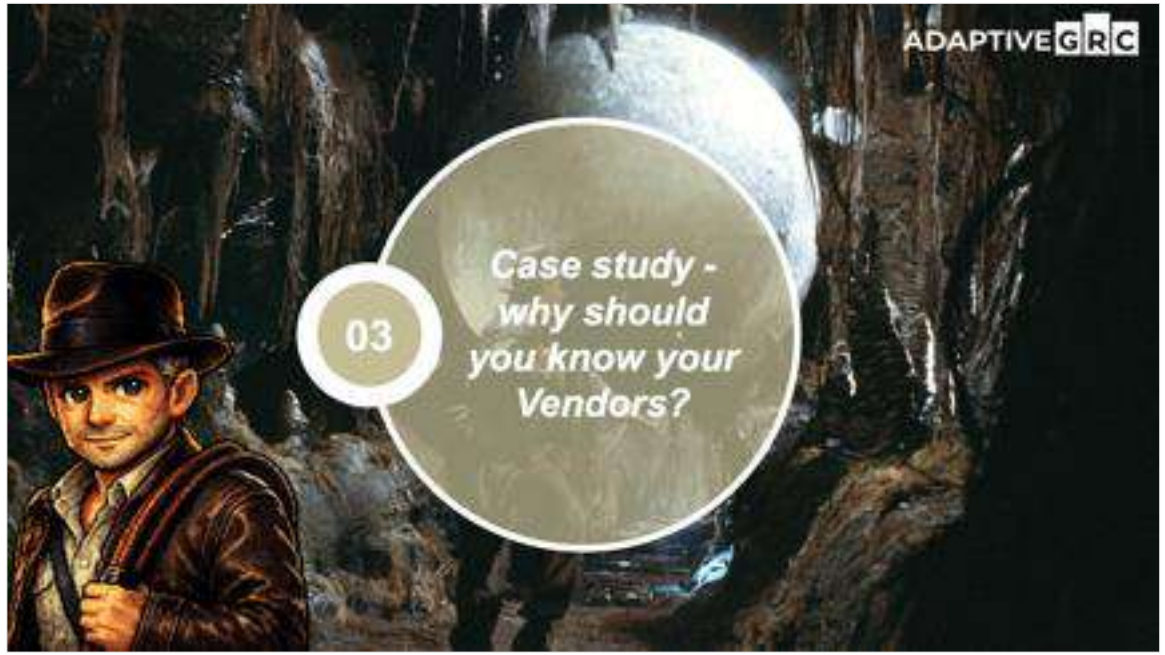
60+ We have improved our skills by implementing IT projects **in over 60 countries** around the world

420+ More than **420 professionals** with the highest qualifications and skills

24/7 **Continuous support** for users whenever they need it


ADAPTIVEGRC
01
Challenges connected with Vendors


ADAPTIVEGRC
02
Recommended steps to ensure Vendor compliance


ADAPTIVEGRC
03
Case study - why should you know your Vendors?

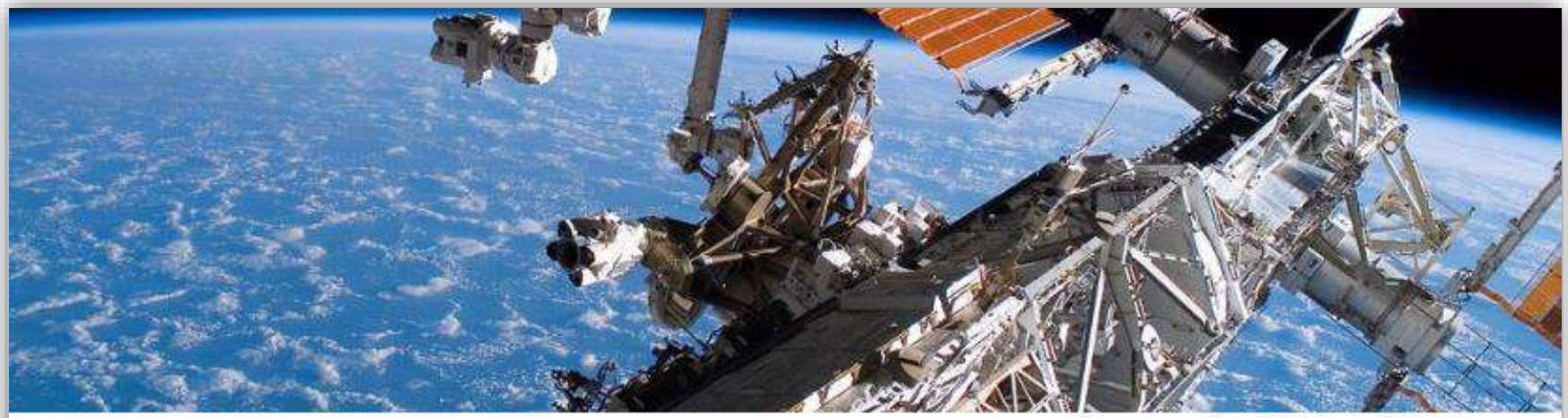

ADAPTIVEGRC
04
Summary

ADAPTIVE GRC

01

Challenges connected with Vendors

FACTS ON THE WALL OF SHAME



Photographer: NASA via Getty Images

Business

NASA Says Metals Fraud Caused $700 Million Satellite Failure

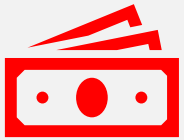
By David Stringer

May 1, 2019, 3:34 AM GMT+2

Updated on May 1, 2019, 11:53 AM GMT+2

CONSEQUENCES

Loss of reputation



Penalties for non-compliance (regulator)

Legal responsibility

Operational / Business Interruptions

WHY DO WE NEED VENDORS / SUBCONTRACTORS?

KEY DRIVERS

WHY DO WE NEED VENDORS/SUBCONTRACTORS?

NASA has contracted with the private sector for most of the services and products it uses.

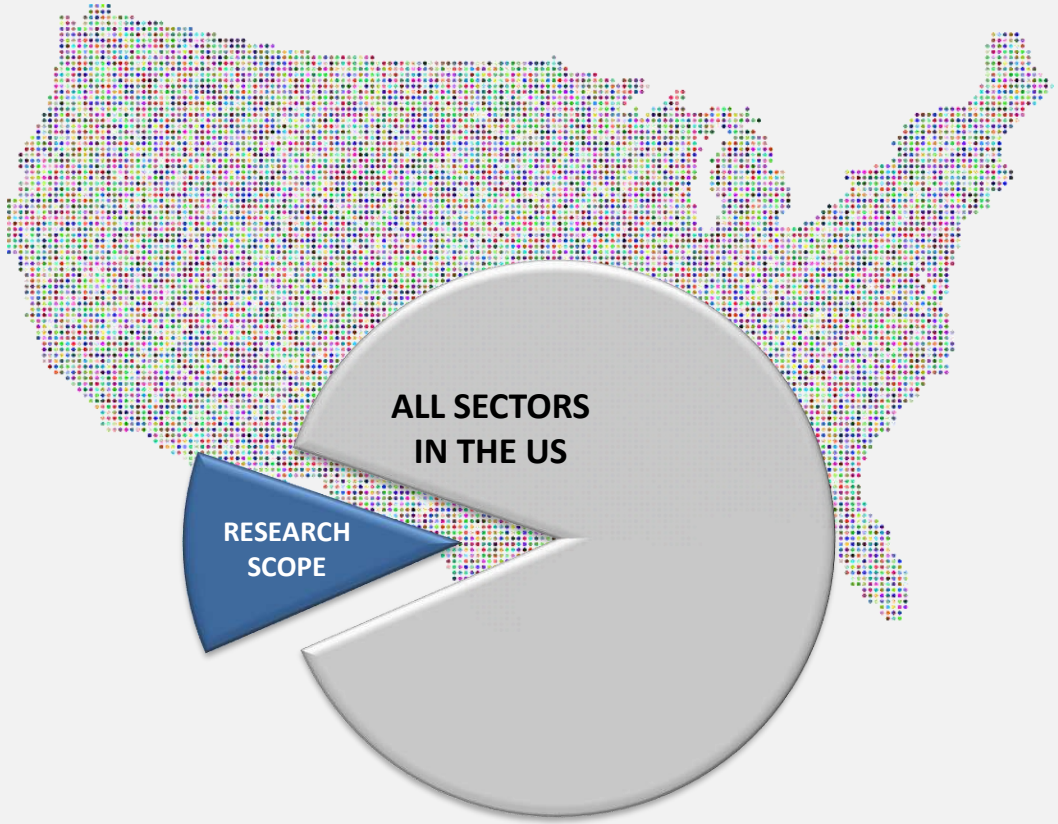
AROUND 400 SUBCONTRACTORS

"The agency had approximately 400,000 talented people who contributed to putting the first human on the Moon," a NASA spokesperson told ClearanceJobs via an email. "According to the figures we have in our collection, NASA had 33,200 federal employees and 377,000 contractors in the mid-1960s."

https://news.clearancejobs.com/2019/07/17/how-government-contractors-helped-send-a-man-to-the-moon-celebrating-apollo-11/

RESEARCH FOCUSED ON THE GRC AND VENDOR MANAGEMENT MARKET IN THE US

Consulting project with UCLA as part of GAP (Global Access Program)



Less than 12%

~30%

CHOSEN CHALLENGES ASSOCIATED WITH VENDORS

OPERATIONAL PERSPECTIVE

HOW TO START TO APPROACH AN EFFICIENT VENDOR RISK MANAGEMENT PROCESS?

Jan Anisimowicz (PMP, CISM, CRISC)

APPROACH

01 *Challenges connected with Vendors*

ADAPTIVE GRC

02

Recommended steps to ensure Vendor compliance

THE RIGHT PATH

- LEWIS CARROLL, ALICE IN WONDERLAND

02 *Recommended steps to ensure Vendor compliance*

ALICE:

WOULD YOU TELL ME, PLEASE, WHICH WAY I OUGHT TO GO FROM HERE?

I DON'T MUCH CARE WHERE.

...SO LONG AS I GET SOMEWHERE.

THE CHESHIRE CAT:

THAT DEPENDS A GOOD DEAL ON WHERE YOU WANT TO GET TO.

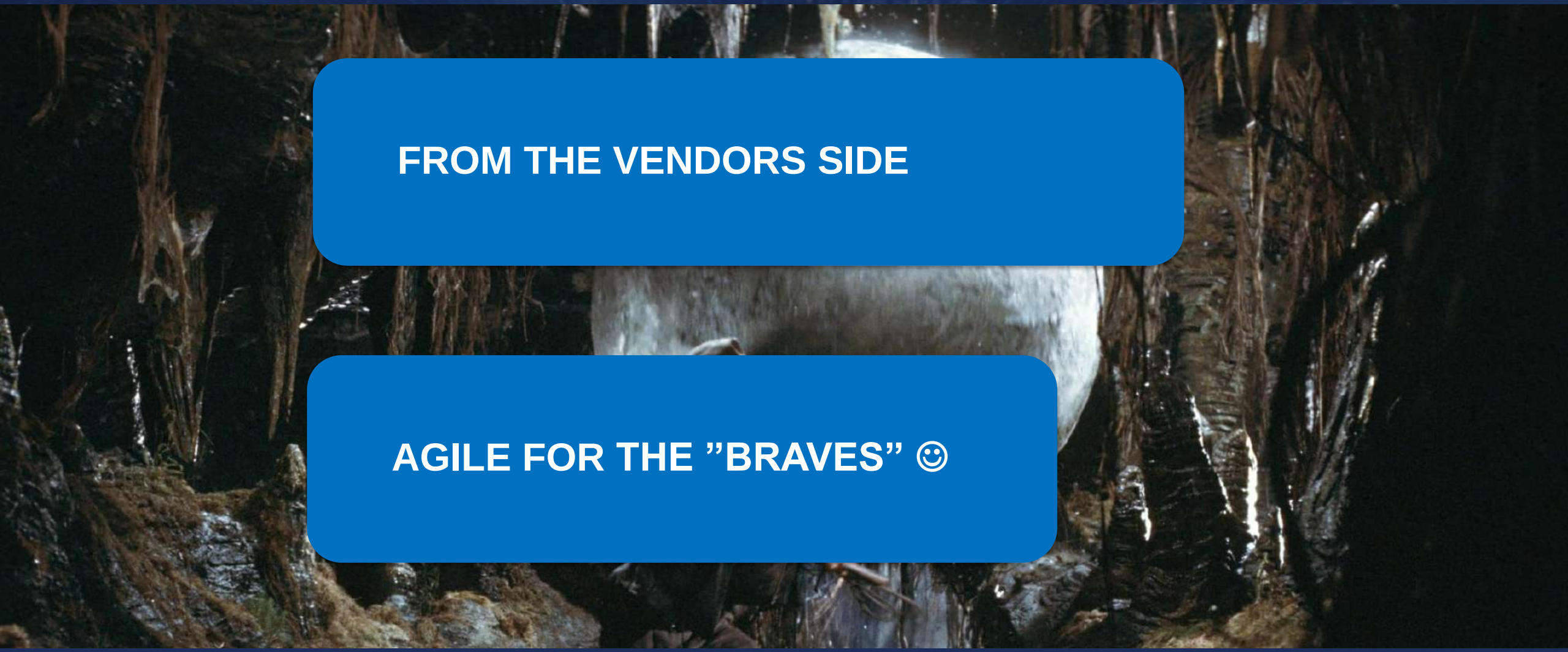
THEN IT DOESN'T MUCH MATTER WHICH WAY YOU GO.

OH, YOU'RE SURE TO DO THAT, IF ONLY YOU WALK LONG ENOUGH.

VENDOR MANAGEMENT PROCESS - APPROACH

02

Recommended steps to ensure Vendor compliance



FROM THE VENDORS SIDE

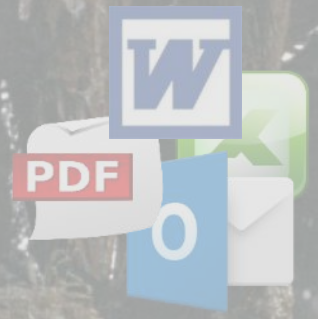
AGILE FOR THE ”BRAVES” ☺

ONE OF THE POTENTIAL WAYS…

AGILE FOR THE ”BRAVES”…

LET’S KEEP OUR FINGERS CROSSED
THAT THIS WILL NEVER HAPPEN AGAIN.

WHATEVER EVIDENCE
IS AVAILABLE



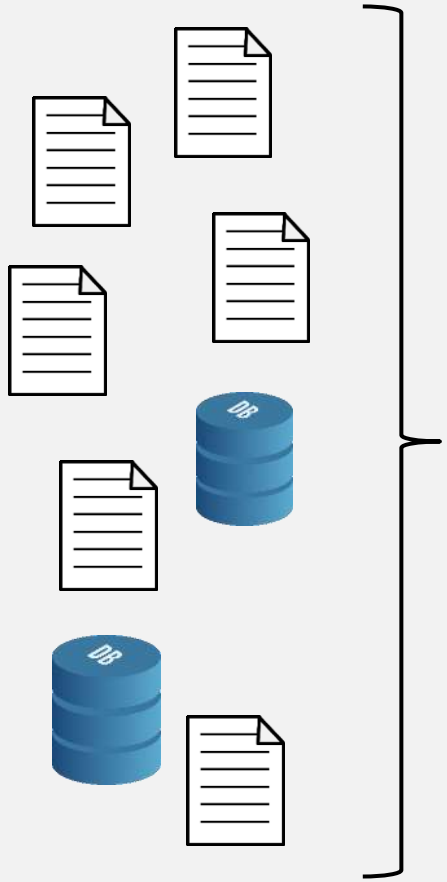
AUDITOR IS AROUND THE CORNER!
!@#$%^

INDIANA JONES APPROACH TO THIRD-PARTY RISK MANAGEMENT in 8 Steps

CREATE / CONSOLIDATE LIST OF VENDORS

02 *Recommended steps to ensure Vendor compliance*

STEP 1



INTERNAL SOURCES

TIP 1

Sometimes this activity would be easier to deliver as part of a Vendor Consolidation Project (costs rationalization in the organization)

Vendor Name	Contact	Email	Address	(…)
C&F LLC	…	…	…	…
AdaptiveGRC SA	…	…	…	…
Audit Masters Inc.	…	…	…	…

TIP 2

It would be helpful to have similar information about all the vendors

CREATE A LIST OF SERVICES THAT YOU CONSIDER RELEVANT TO YOUR ORGANIZATION

STEP 2

- **Outsourced business functions** (IT services, Accounting, cleaning service)
- Subcontracting
- Data hosting
- Data processing
- System Maintenance
- Pizza delivery service
- Cloud applications
- Transportation
- Facilities Management
- And many, many more …

TIP 3

In the long run, it would be beneficial for the organization to have a hierarchy of services

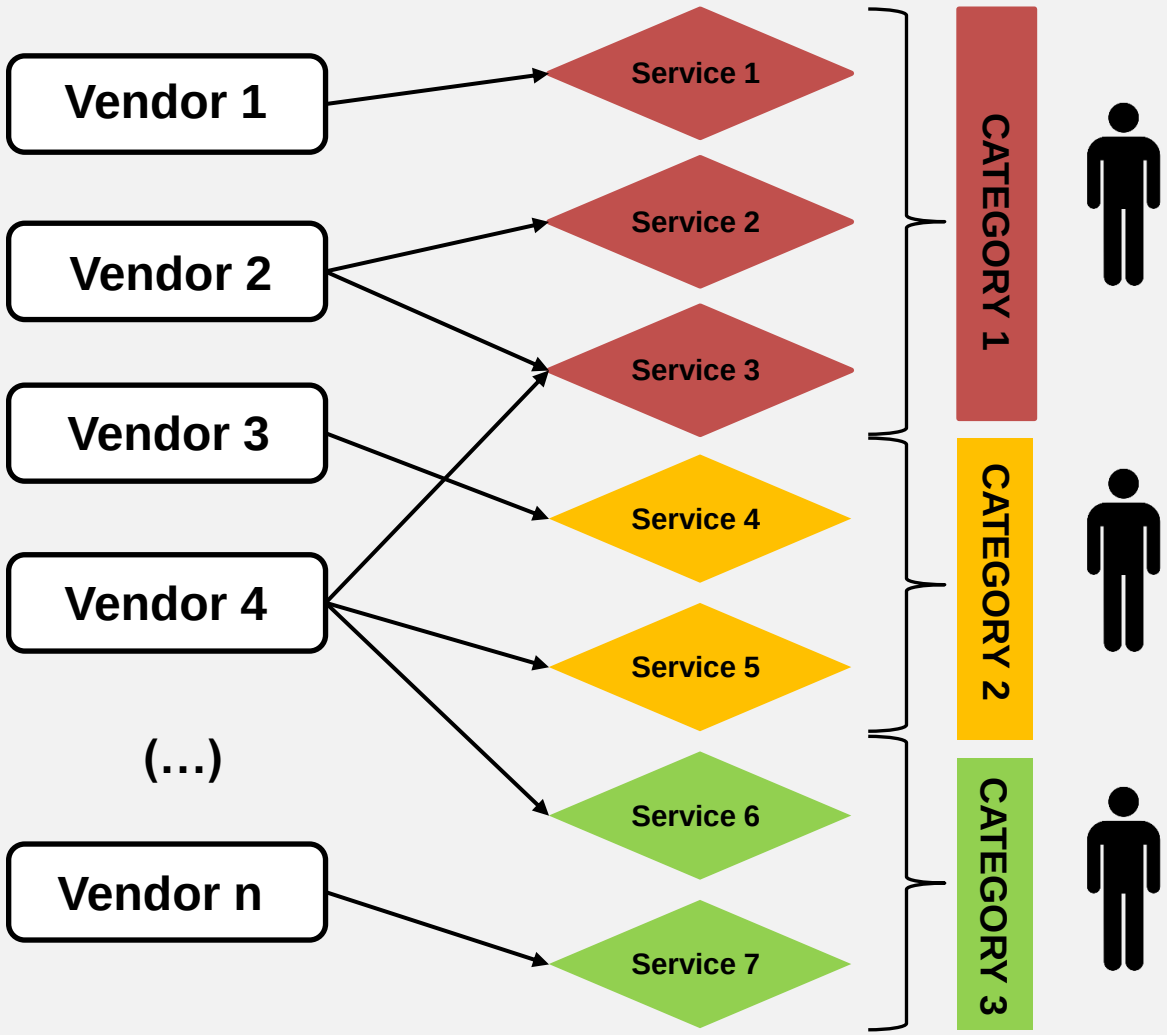
TIP 4

It would be useful to assign importance of the service for the organization

MAKE THE RELATIONS BETWEEN VENDORS AND SERVICES

02 *Recommended steps to ensure Vendor compliance*

STEP 3



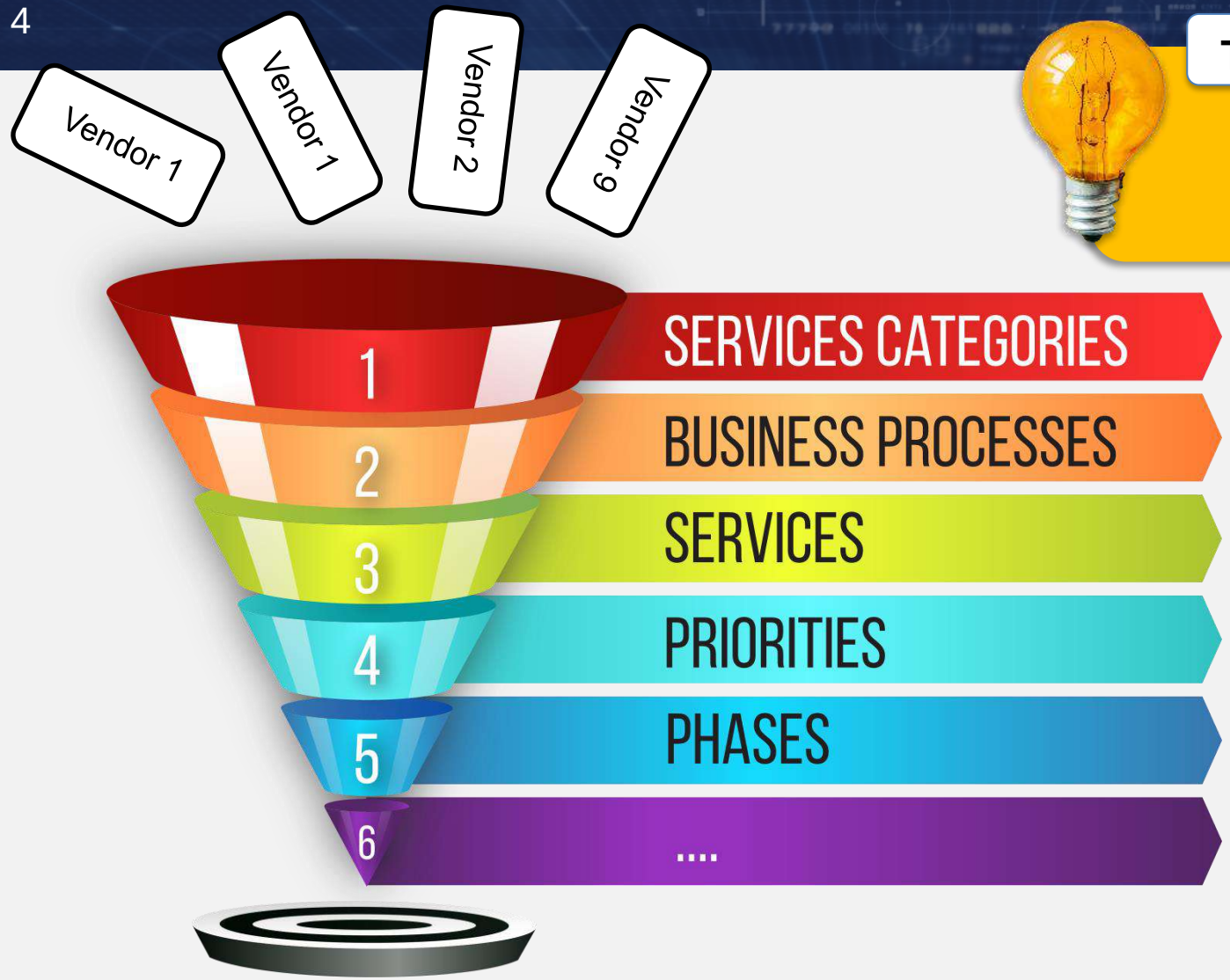
TIP 5

Based on the categorization you can assign business responsibility to different colleagues in the organization (better buy-in process).

VERIFY THE NEED FOR CREATING VENDOR RISK PROFILES

02 *Recommended steps to ensure Vendor compliance*

STEP 4



TIP 6

Filtering criteria should be harmonized in the organization. No exceptions.

CREATE A VENDOR RISK PROFILE

STEP 5

02 *Recommended steps to ensure Vendor compliance*

SERVICES RISKS:

- ★ Compliance and regulatory risks related to the service
- ★ Customer and financial impact
- ★ Criticality level of the service delivered by the vendor for our company
- ★ Financial transactions processed
- ★ Personal and sensitive data involved?
- ★ Maturity of the service?
- ★ ...

ENTITY RISKS:

- ★ Location of the vendor
- ★ Known security incidents
- ★ Size of the company
- ★ Financial standings
- ★ Performance history
- - …

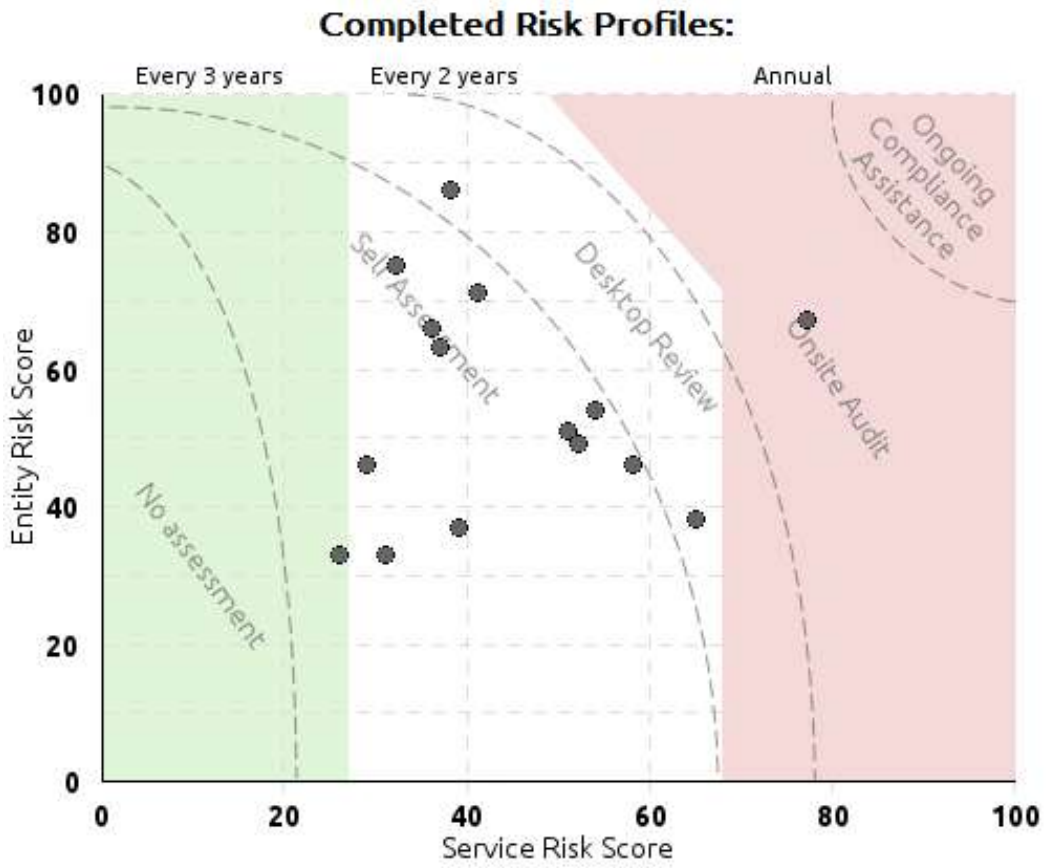
TIP 7

You have to leverage knowledge available in your organization (it's a MUST). You can enrich the data with additional information sources (like D&B, Bisnode etc.)

CREATE A VENDOR RISK PROFILE (SUMMARY)

02 *Recommended steps to ensure Vendor compliance*

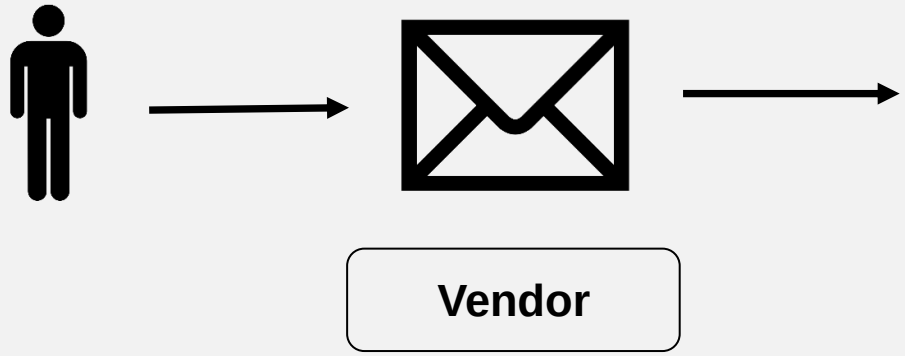
STEP 5 EXAMPLE



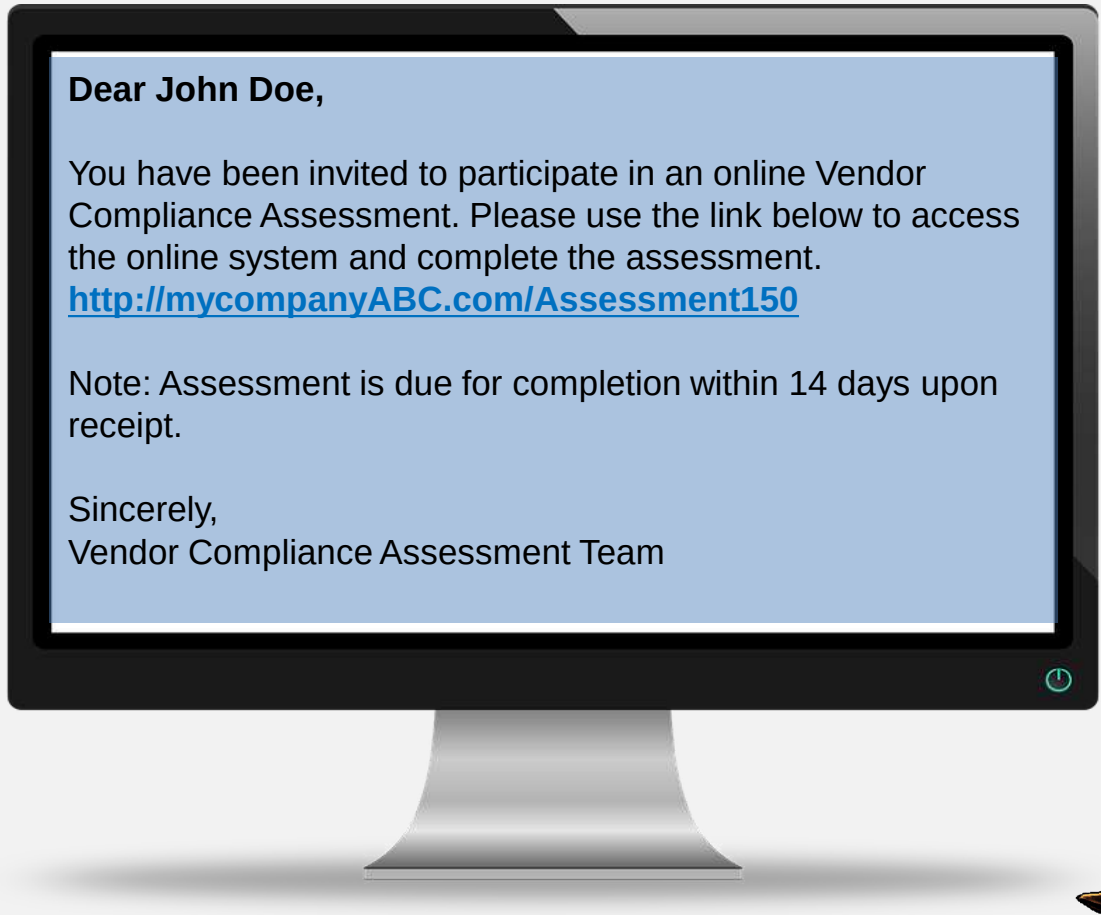
CHECK THE VENDOR COMPLIANCE AND ASSESS RISKS USING A SELF-ASSESSMENT

STEP 6

02 *Recommended steps to ensure Vendor compliance*



Vendor



RECOMMENDATION

STEP 6

02 *Recommended steps to ensure Vendor compliance*

Preview Assessment results

Objective Id	Activity Group Parent	Activity Group	Compliance Objective	Risk Rating	Response
COB101	Information Protection	Media Security	Whenever physical media containing sensitive or regulated data is moved between locations, a movement log must track and verify that the media safely reaches the required destination and custodian.	Critical	Yes
COB141	Information Protection	Incident Management	All reported events must be captured in a secure incident log or incident management system with the following information: • date and time of event • location, systems and information affected • disposition of event: classified as incident or non-incident with rationale • containment, notification and recovery outcomes. • the information/data owner	Very High	Yes
COB120	Information Protection	Information Security Management	The organization must have a documented Information Security policy. The contents of the policy includes (but is not limited to): - The identification of a single individual as the head of Information Security, with overall accountability for delivery of the information security objectives. - The organizations high-level commitment, sponsorship and strategy to assure the ongoing protection of information. - A commitment to assure that information security training is provided to all appropriate resources.	Critical	No
COB121	Information Protection	Information Security Management	The security policy of the Service Organization must state that networks are required to be protected from unauthorized access and also identify the network availability requirements. The network availability and integrity requirements must comply with prevailing contractual and regulatory requirements.	Critical	Partial
COB124	Information Protection	Data Exchange	All software and data imports from a non trusted source must be checked for viruses and verified as clean before being made available in the organizations network or systems.	Critical	No
COB126	Information Protection	Information Security Management	Normal operational access privileges to workstations must prevent unauthorized software from being installed. Unauthorized software includes, but is not limited to, any software that can facilitate unauthorized access into any part of the organizations network. Installation of software without a valid software license is also prohibited.	Very High	Yes

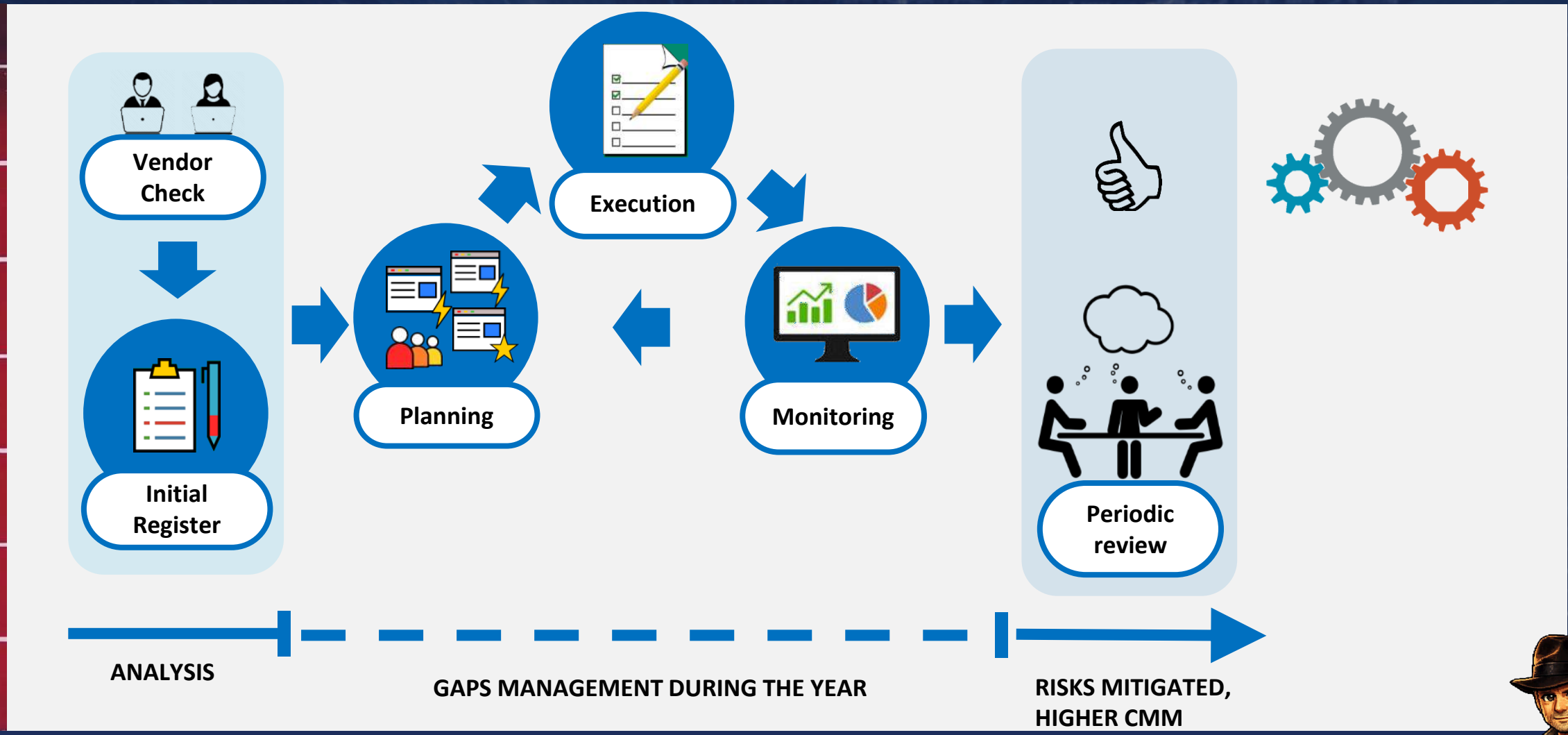
HOW ABOUT

GAPS AND FINDINGS MANAGEMENT?

GAPS AND FINDINGS MANAGEMENT

STEP 7

02 *Recommended steps to ensure Vendor compliance*

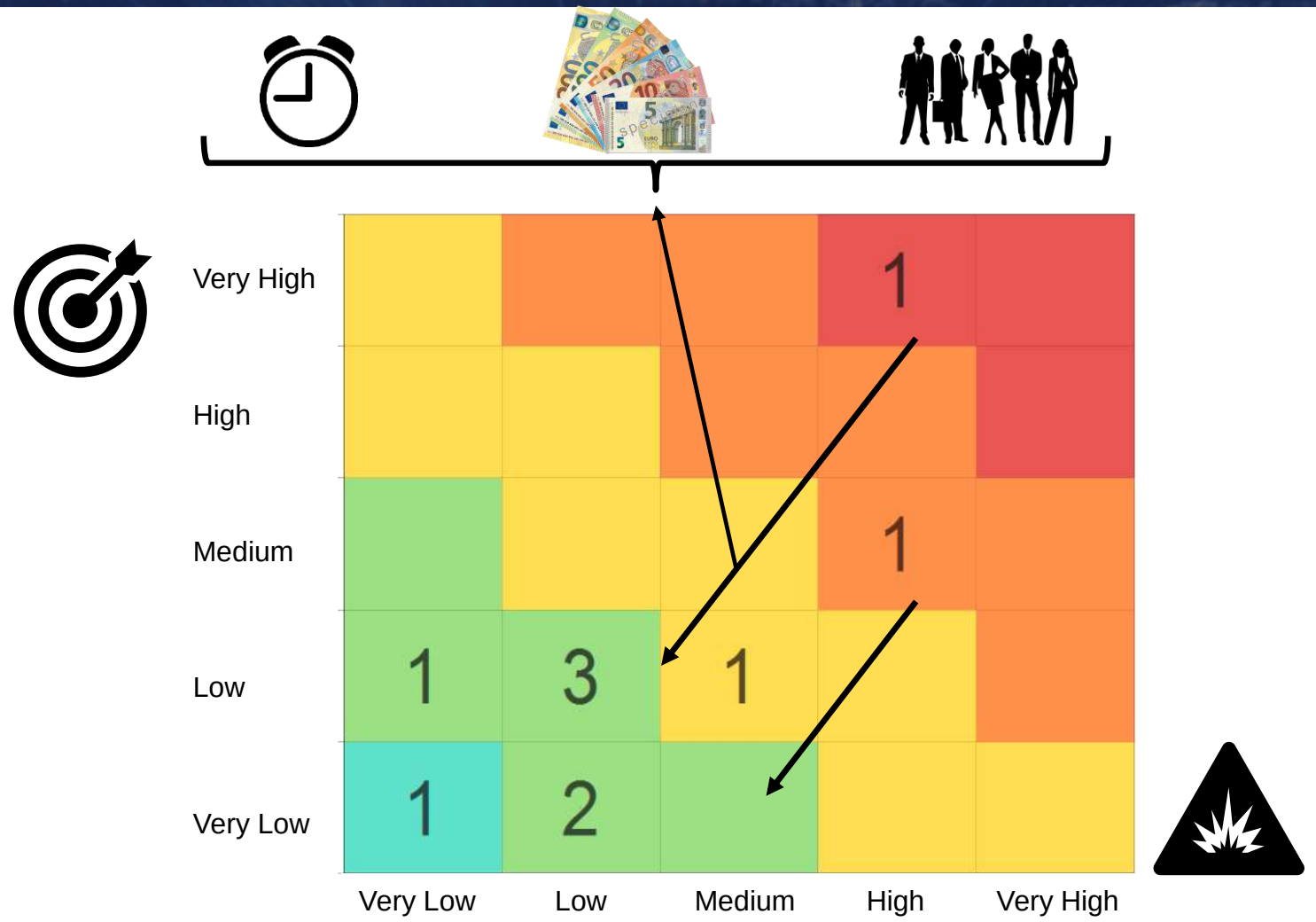


Jan Anisimowicz (PMP, CISM, CRISC)

RISKS MITIGATION TO IDENTIFIED FINDINGS (PROBABILITY/IMPACT MATRIX)

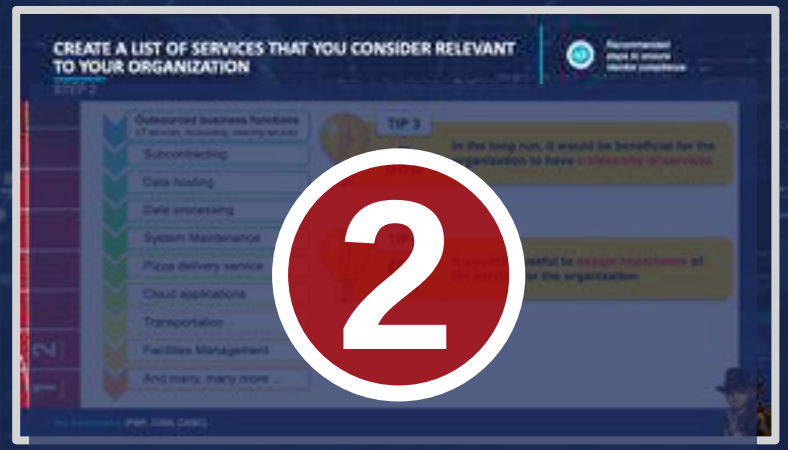
STEP 8

02 *Recommended steps to ensure Vendor compliance*




INDIANA JONES APPROACH TO THIRD-PARTY
RISK MANAGEMENT in 8 Steps
1 2 3 4 5 6 7 8


CREATE / CONSOLIDATE LIST OF VENDORS
STEP 1
1


CREATE A LIST OF SERVICES THAT YOU CONSIDER RELEVANT TO YOUR ORGANIZATION
2


MAKE THE RELATIONS BETWEEN VENDORS AND SERVICES
Vendor 1
Vendor 2
Vendor 3
Vendor 4
Vendor n
3


VERIFY THE NEED FOR CREATING VENDOR RISK PROFILES
4

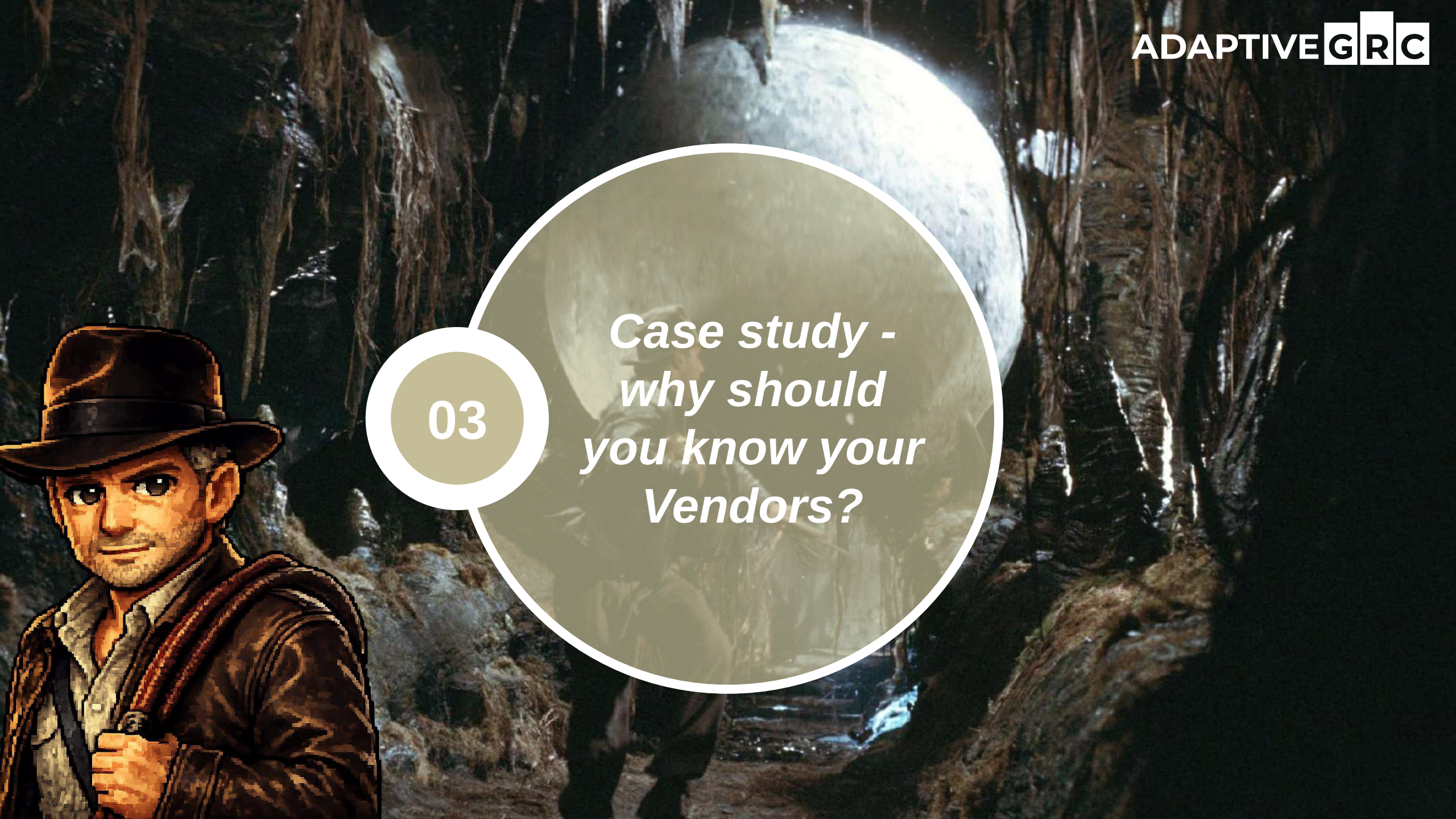

CREATE A VENDOR RISK PROFILE (SUMMARY)
5


RECOMMENDATION
STEP 6
6


GAPS AND FINDINGS MANAGEMENT
STEP 7
Vendor Check
Initial Register
Periodic review
ANALYSIS
RISKS MITIGATED, HIGHER CMM
7


RISKS MITIGATION TO IDENTIFIED FINDINGS (PROBABILITY/IMPACT MATRIX)
STEP 8
8

ADAPTIVE GRC



03

Case study - why should you know your Vendors?

CASE STUDY

03 *Case study - why should you know your Vendors?*

CASE STUDY

CASE STUDY – BATTLE OF BRITAIN - 1940

IN A NUTSHELL

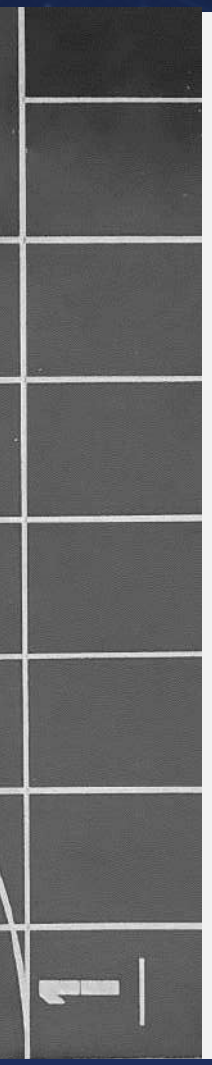
Royal Air Force Benevolent Fund

BATTLE OF BRITAIN
10 JULY – 31 OCTOBER 1940

BATTLE OF BRITAIN

BATTLE OF BRITAIN - VENDOR RISK PROFILE AND ASSESSMENT

STEP 1: Create / Consolidate list of Vendors



VENDORS FROM 15 COUNTRIES

- POLAND
- NEW ZEALAND
- CANADA
- CZECHOSLOVAKIA
- BELGIUM
- AUSTRALIA
- SOUTH AFRICA
- FRANCE
- IRELAND
- UNITED STATES
- SOUTH RODESIA
- JAMAICA
- BARBADOS
- NEWFOUNDLAND
- NORTHERN RHODESIA

BATTLE OF BRITAIN - VENDOR RISK PROFILE AND ASSESSMENT

STEP 2: Create a list of services that you consider relevant to your organization

SERVICE:

- Fighter Pilots (FP)
- Bomber Pilots (BP)

BATTLE OF BRITAIN - VENDOR RISK PROFILE AND ASSESSMENT

STEP 3: Make the relations between Vendors and Services

VENDOR:

Poland

SERVICES:

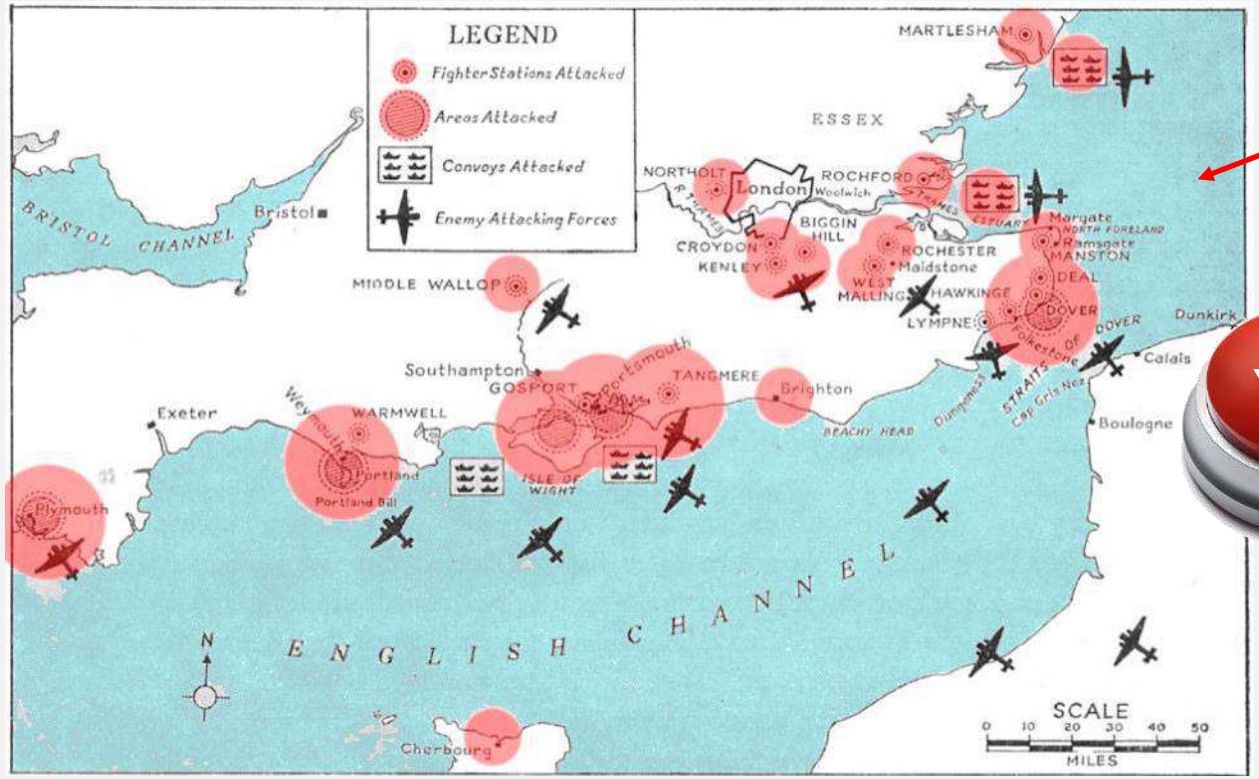
88 Fighter Pilots (FP)

57 Bomber Pilots (BP)

BATTLE OF BRITAIN - VENDOR RISK PROFILE AND ASSESSMENT

STEP 4: Verify the need for creating Vendor Risk Profiles

IS THIS SERVICE IMPORTANT FOR US?



BATTLE OF BRITAIN - VENDOR RISK PROFILE AND ASSESSMENT

STEP 5: Create a Vendor Risk Profile

VENDOR RISKS PROFILES

Vendor Risk Profile (Polish Pilots):

- ☒ They do not know British combat tactics
- ☒ They do not have experience with modern planes (Hurricanes, Spitfires)
- ☒ Insufficient command of English

BATTLE OF BRITAIN - VENDOR RISK PROFILE AND ASSESSMENT

STEP 5: Create a Vendor Risk Profile

VENDOR RISKS PROFILES

Vendor Risk Profile (Polish Pilots):

- ☒ They do not know British combat tactics
- ☒ They do not have experience with modern planes (Hurricanes, Spitfires)
- ☒ Insufficient command of English
- ☒ Too eager to fight with the enemy …


Bandits! Bandits! Beneath us!
On the right!

BATTLE OF BRITAIN - VENDOR RISK PROFILE AND ASSESSMENT

STEP 6: Check the vendor compliance and assess risks using a self-assessment

ASSESSMENT (DURING THE BATTLE).

- Extremely Good Pilots
- Broad battle experience
- Direct fight tactics better than expected **(5 to 1)**
- Incredibly efficient

On the first mission of the 303 Squadron, six enemy fighter planes were shot down. In 15 minutes.

BATTLE OF BRITAIN - VENDOR RISK PROFILE AND ASSESSMENT

STEP 7: GAPs and Findings management

STEP 8: Risks Mitigation to identified findings

NOT REQUIRED, LET THEM FLY

BATTLE OF BRITAIN - VENDOR RISK PROFILE AND ASSESSMENT

03

Case study - why should you know your Vendors?

Jan Anisimowicz (PMP, CISM, CRISC)

ADAPTIVE GRC

04

Summary

VENDOR MANAGEMENT IMPLEMENTATION APPROACH

ADAPTIVE GRC

RISK MANAGEMENT

1. Enterprise Risk Module
2. Quality Module

INTERNAL CONTROL

1. Content Module
2. Regulations
3. Internal Control
4. Quality Module

COMPLIANCE MANAGEMENT

1. Content Module
2. Compatibility Module
3. Quality Module
4. 3rd party vendor risk

INTERNAL AUDIT

1. Organization Module
2. Internal Audit Module
3. Quality Module

Common process space and organizational structure

Connects all modules and allows you to share data for other systems

Our Special Offer for Audit Masters 2026

PROMO CODE

AdaptiveGRC_AuditMasters

Try AdaptiveGRC today with our limited-time offer

Free internal audit training (GRC tool usage)

3 months free access to Internal Audit module (up to 3 users)

- Feel free to forward the QR code to friends and colleagues.
- Scan the QR code to sign up and discuss details or visit us at our booth.

SIGN UP VIA QR-CODE

Offer valid until June 30, 2026

IMPORTANT QUESTION...

Do You Know the Path?


THERE'S A DIFFERENCE
BETWEEN KNOWING THE PATH

THANK YOU!

Thank You
For Your
Attention

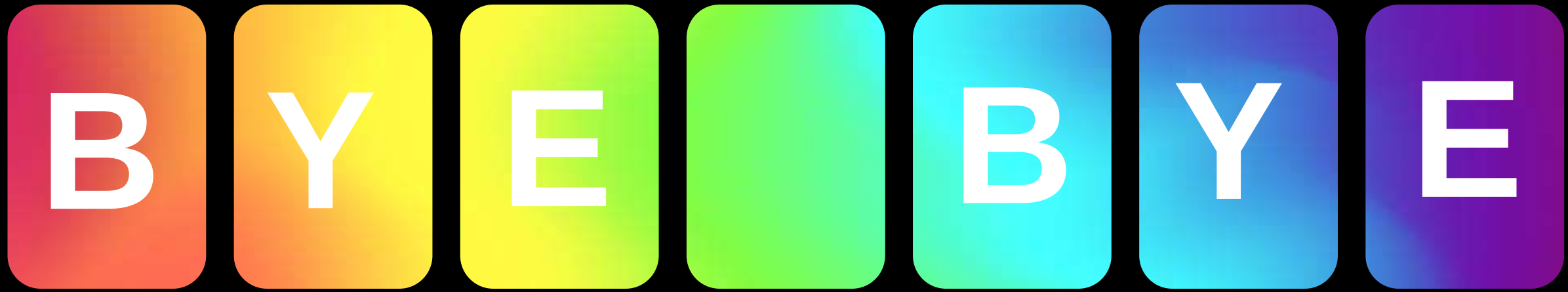
Thank you for your attention!

Jan Anisimowicz

Board Member, C&F SA Poland

AdaptiveGRC product

Jan.Anisimowicz@candf.com


BYE BYE