KB4-CON

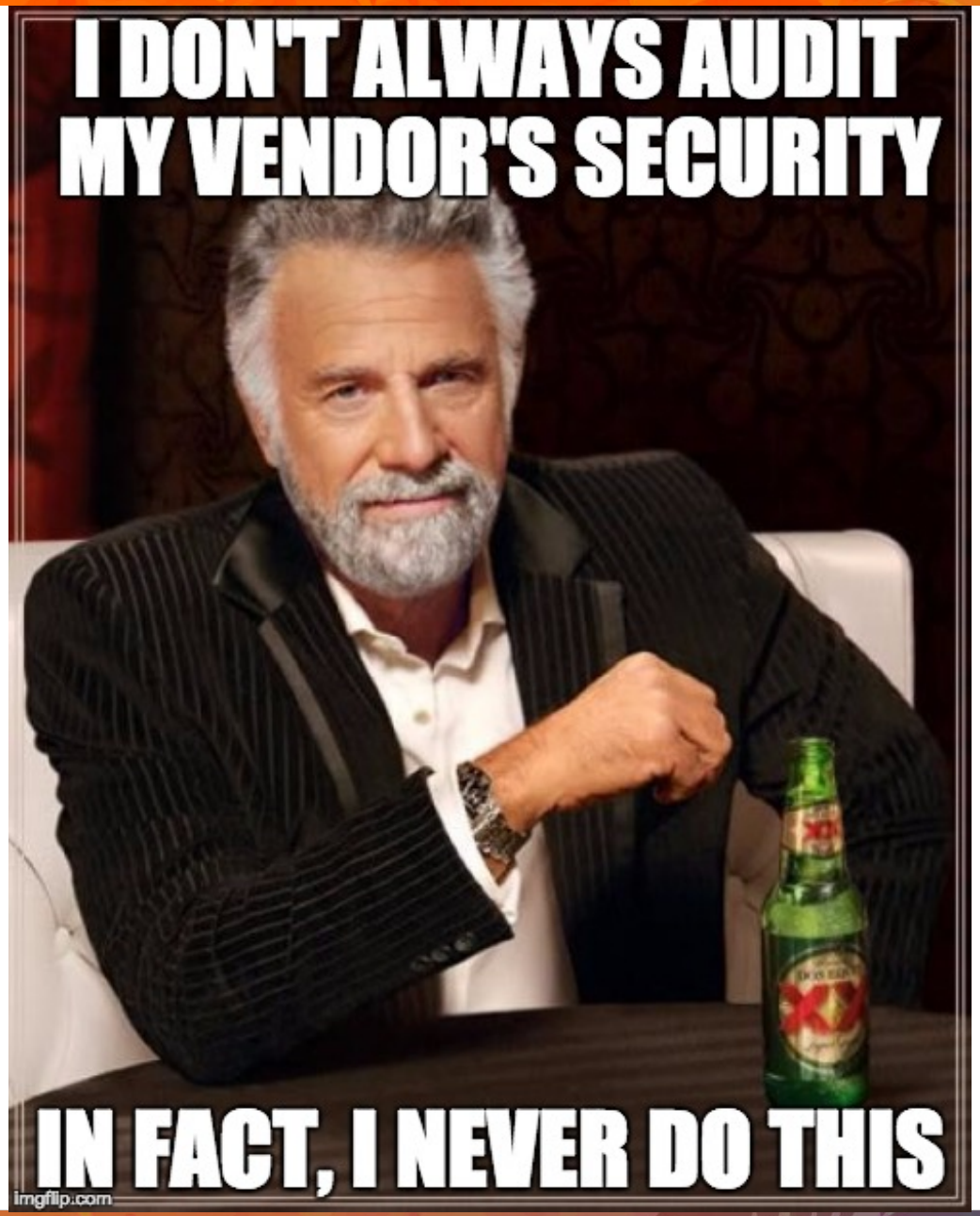
New School Third Party Risk Management

by Brian Jack, CISO, DPO, CISSP, CEH, AWS/Security Specialist
and Lecio de paula, FIP, CIPP/US, CIPP/E, CIPP/C, CIPM

KnowBe4

What we are going to talk about

- What is third party/vendor risk
- Conducting risk assessments
- Cloud/SaaS vendor risk specifics
- Streamlining due diligence process
- Red flags/lessons learned


I DON'T ALWAYS AUDIT
MY VENDOR'S SECURITY
IN FACT, I NEVER DO THIS
imgflip.com

Why is third party risk management important?

- Reduce likelihood of data breaches
- Fulfill legal obligations
- Ensure vendors can meet expected SLA's
- Business continuity and contingency planning (critical vendor merger or bankruptcy)
- Regulatory compliance

The ultimate goal is to protect your data and CYA!

What are the types of third party risk?

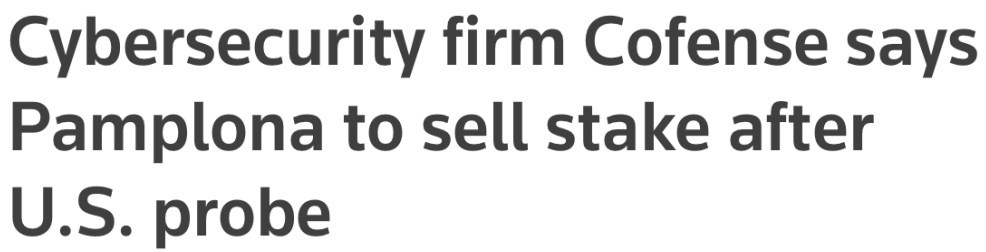
- **Compliance risk** is related to violations of laws, rules, or regulations

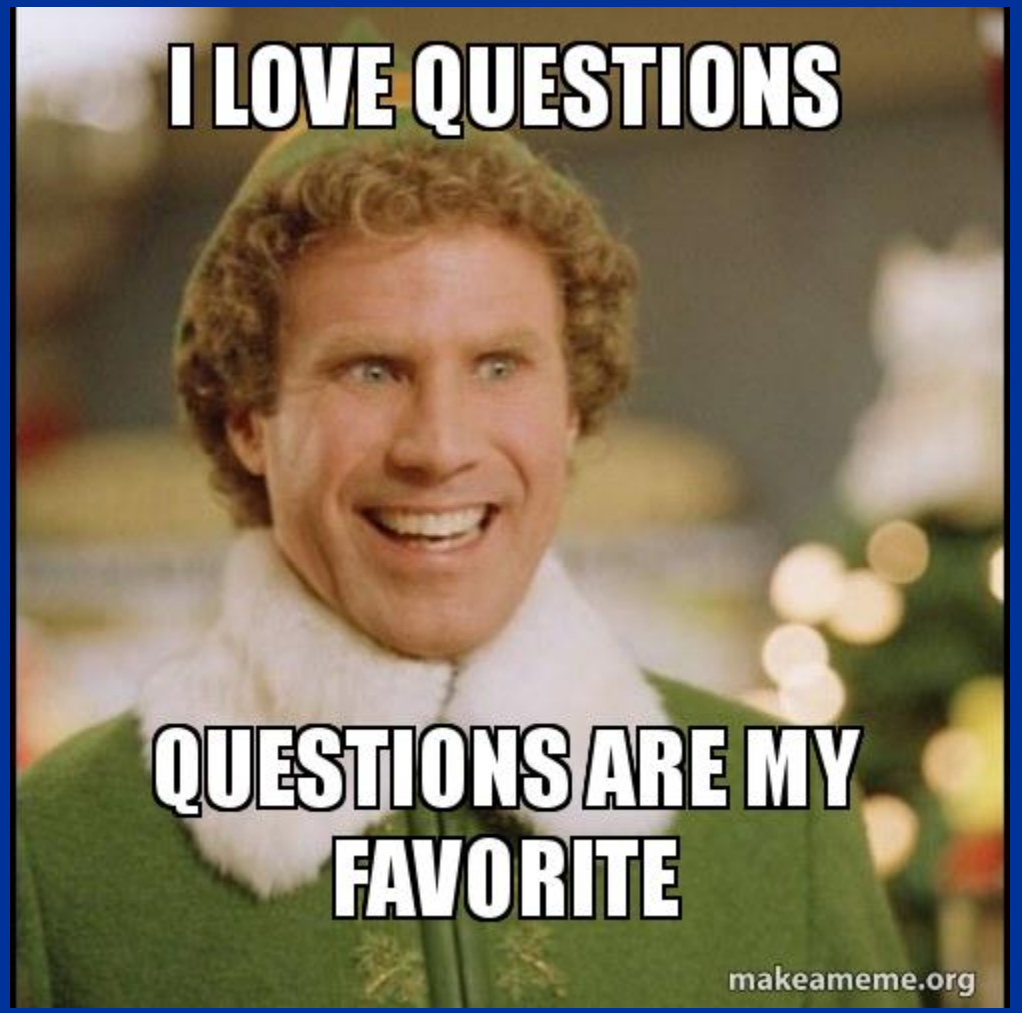
  (**GDPR, HIPAA, and others**)

- **Strategic risk** business decisions not in line with strategic goals

- **Transactional risk** is related to problems with service or product delivery.

- **Reputational risk** is related to negative public opinion (re: Cofense and Russian money)





Key Questions

1. Do they need access to our systems or network?
2. What data are we sharing with them?
3. Where will this data be stored, and for how long?
4. What third party vendors do they use (fourth party risk)?
5. What supporting evidence do they have?

How can these questions be answered?

Do they need access to our systems or network?

- Do they require a user account (if so what permissions)?
- Do they require access to the network?
- Example: WIPRO, Target

What data are we sharing with them?

- Employee data? Customer Data? Company Confidential Information?
- PCI Data? Health Information? Regulatory compliance risk?

Image courtesy of edps.com

HIPAA

Image courtesy of hhs.gov

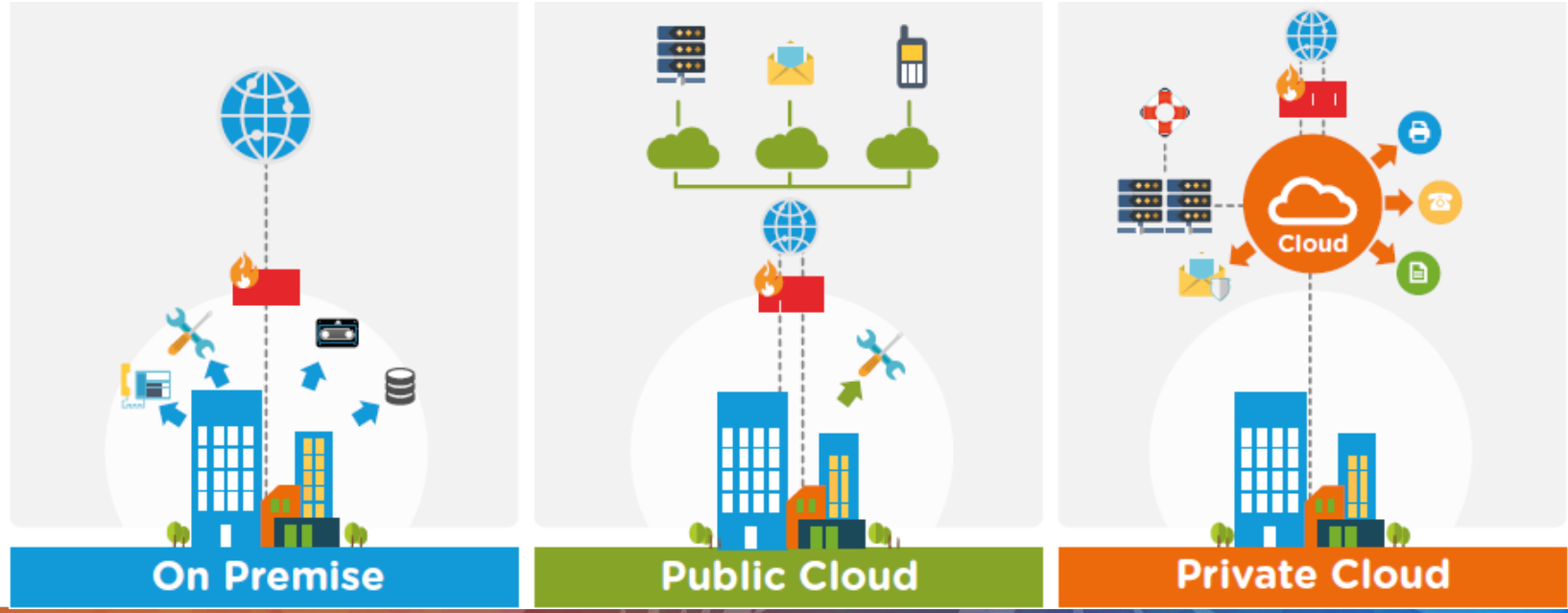
PCI Security Standards Council

Image courtesy of pcisecuritystandards.org

Where will the data be stored and for how long?

- Will there be cross border transfer? US, EU? Others?

- Legal or regulatory requirements?
- Vendor should only store data as long as necessary to provide its services.



Source: EBC Group

What third party vendors do they use? (fourth party risk)

Image courtesy of Upguard.com

- Ensure standards no less stringent than those imposed on your vendors are imposed on the fourth party (by way of contract)
- Request evidence of proper due diligence of fourth parties

What supporting evidence do they have?

- Report from independent audit
- Vulnerability scans and penetration tests
- DRP/BCP tests
- Compliance reports (AWS Trusted Advisor)

Source: EBC Group

Essential elements of third party due diligence

- Third-party reviews (SOC 2, ISO, etc.)
- Documentation on the provider's information security and business continuity programs
- DPIA's (Data Privacy Impact Assessments)
- Vendor history (service interruptions, security breaches, legal or regulatory issues, etc.)
- Security questionnaires (CAIQ, SIG, HECVAT etc.)
- Financial stability statements

Cloud specific risks

- Now more than ever it's necessary to perform due diligence on cloud based vendors not just *of* the cloud provider, but also the architecture *in* the cloud
- Questionnaires alone are insufficient and the real action is happening *in* the cloud
- How do you know if your vendor is using the cloud in line with best practices?

e.g. Booz Allen Hamilton, Verizon leaky cloud storage


NICE BUCKET YOU HAVE THERE
SHAME IF SOMETHING HAPPENED TO IT
imgflip.com

Booz Allen Hamilton

When: May 2017

Data Exposed: Battlefield imagery and administrator credentials to sensitive systems

The Lowdown: The U.S. defense contractor left data publicly accessible through an insecurely configured S3 account containing files related to the National Geospatial-Intelligence Agency (NGA), which handles battlefield satellite and drone imagery. Booz Allen claims the data itself was not connected to classified systems, but included in the data were remote login keys and credentials that could have been used to access more sensitive data.

Dow Jones & Co

When: July 2017

source: threatpost.com

Data Exposed: Personally identifiable information for 2.2 million people

The Lowdown: Wall Street Journal parent company Dow Jones & Co exposed personal information about more than 2 million customers through sloppy S3 configuration. In this case, permissions were set to allow anyone with a free AWS account access to a server containing millions of customer account details, as well as another database containing consumer data about millions of people for anti-money laundering regulatory compliance purposes.

Image courtesy of infosecurity-magazine.com

Security “in” the cloud

Source google.com

Source amazon.com

Source microsoft.com

- Request appropriate reports for security in the cloud
- **Amazon AWS** - Trusted Advisor Reports
- **Microsoft Azure** - Azure Advisor and Azure Security Score
- **Google Cloud** - Summary of Security Platform
- OR reports from third party cloud security applications containing similar information

Security

8 7 2

Filter by tag

Tag Key | Tag Value | Apply filter | Reset

View: No problems detected

Security Checks

Amazon EBS Public Snapshots

Checks the permission settings for your Amazon Elastic Block Store (Amazon EBS) volume snapshots and alerts you if any snapshots are marked as public.

0 EBS snapshots are marked as public.

Amazon RDS Public Snapshots

Checks the permission settings for your Amazon Relational Database Service (Amazon RDS) DB snapshots and alerts you if any snapshots are marked as public.

0 RDS snapshots are marked as public.

AWS CloudTrail Logging *Refreshed: 6 days ago*

Checks for your use of AWS CloudTrail.

0 of 32 regions or trails are not logging activity.

CloudFront Custom SSL Certificates in the IAM Certificate Store *Refreshed: 6 days ago*

Checks the SSL certificates for CloudFront alternate domain names in the IAM certificate store and alerts you if the certificate is expired, will soon expire, uses outdated encryption, or is not configured correctly for the distribution.

0 of 0 custom SSL certificates are expired, will soon expire, or are incorrectly configured.

[redacted]

B

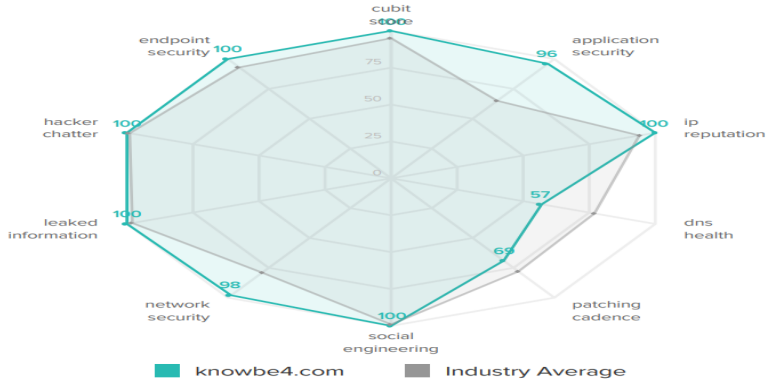
85
current percentile

KnowBe4
TECHNOLOGY
knowbe4.com

Threat Indicators

A 98	**Network Security**	*Detecting insecure network settings.*
F 57	**DNS Health**	*Detecting DNS insecure configurations and vulnerabilities.*
D 69	**Patching Cadence**	*Out of date company assets which may contain vulnerabilities or risks.*
A 100	**Endpoint Security**	*Measuring security level of employee workstations and mobile devices.*
A 100	**IP Reputation**	*Detecting suspicious activity, such as malware or spam, within your company network.*
A 96	**Application Security**	*Detecting common website application vulnerabilities.*
A 100	**Cubit Score**	*Proprietary algorithm checking for implementation of common security best practices.*
A 100	**Hacker Chatter**	*Monitoring hacker sites for chatter about your company.*
A 100	**Information Leak**	*Potentially confidential company information which may have been inadvertently leaked.*
A 100	**Social Engineering**	*Measuring employee awareness to a social engineering or phishing attack.*

Industry Comparison



Vulnerabilities

Vulnerability Type	Measure
Open Ports	0
Site Vulnerabilities	26
Malware Discovered	0
Leaked Information	0

Be reasonable and streamline the process

- Don’t impose unreasonable standards on vendors
  - If vendor has a due diligence package, use it!

- Take into account the nature, risk and scope of processing to ultimately decide what to request from the vendor as well as the obligations to impose by way of contract

What we have seen….

CFR Part 471, Appendix A to Subpart A), relating to the notice of employee rights under federal labor laws.

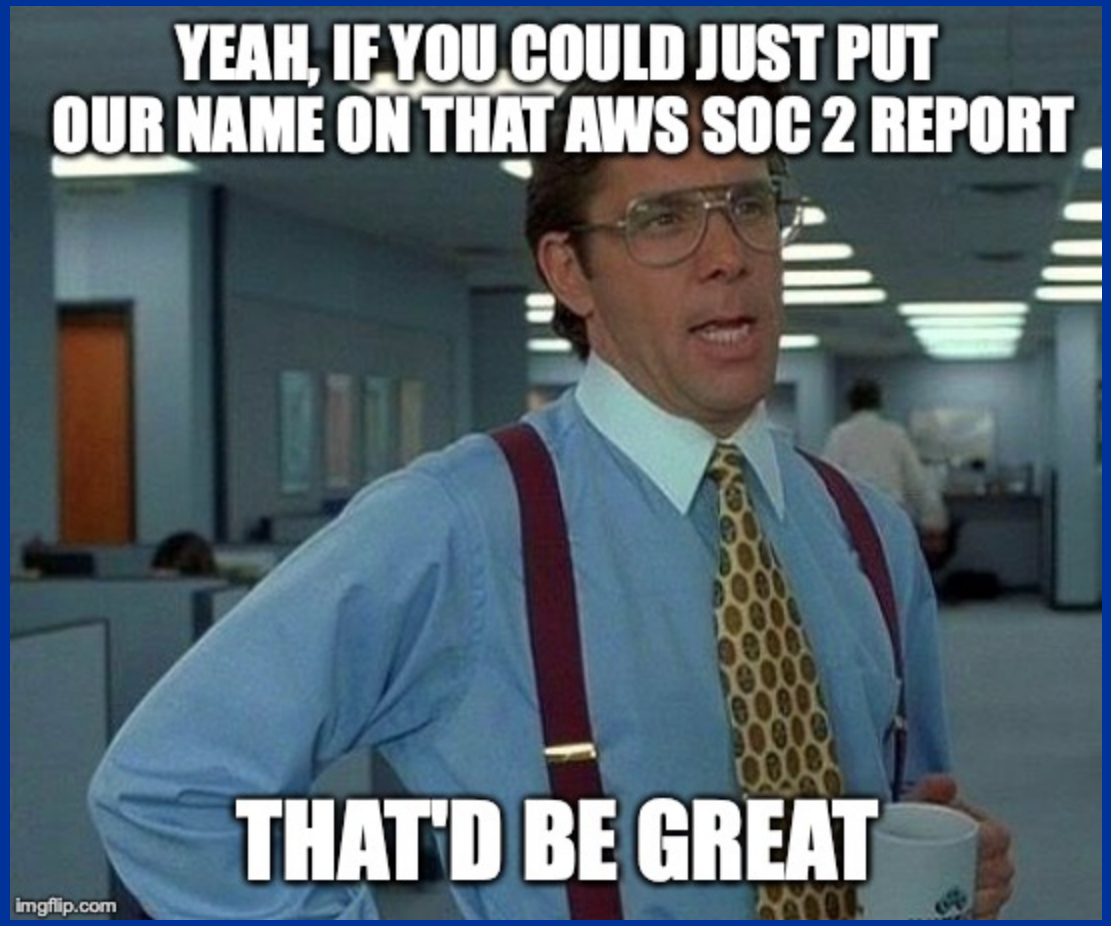
10.2. Supplier Code of Conduct. Supplier will comply at all times with the then-current version of the Supplier Code of Conduct. The terms of the Supplier Code of Conduct, including as it may be subsequently amended, are incorporated in this Agreement by reference. Supplier will promptly report [redacted] discovered or suspected fraud, illegal activity or other violation of the Supplier Code of Conduct.

Appropriate contracts for you and for them

- Work with your legal department to draft the appropriate contracts to execute with third parties
- Data Security Addendums
- Data Processing Agreements or Data Privacy Addendum (Required for GDPR and other data protection legislation). Comprehensive and has the ability to cover both privacy and security obligations.
- Automation where possible

What are some third party RED FLAGS?

Lets go over a few examples



Red Flags!

1. Pass off infrastructure SOC report as their own (i.e. pass off Amazon AWS or Azure SOC Report as their own)

*Vendors are still responsible for security IN the cloud

2. No recent penetration tests or vulnerability scans

[redacted]

to m[redacted]

Are we not able to utilize AWS' SOC 2 in lieu of ours until it's available?

[redacted]

> [redacted] *Subprocessor is AWS, which a very well-known sub processor. Also, industry standard is that SOC by pertinent subprocesors is acceptable.* [redacted]

---------- Forwarded message ---------

[redacted]

Date: Tue, Dec 11, 2018 at 1:09 PM

Subject: Re: [redacted] - SOC 2 Type 2 Report

[redacted]

Good afternoon Ms. [redacted]

[redacted] SOC 2 Type 2 report is available via this link: [redacted]/resources/azure-soc

Please let us know if you have any difficulty accessing it.

Sincerely,

[redacted]

Red Flags (ctd..)

- Old SOC reports without an appropriate bridge letter
- Not willing to execute security or privacy agreements
- History of data breaches
- No documented Infosec & Privacy Policies
- Critical vulnerabilities not remediated in timely fashion or refuse to provide penetration tests and vulnerability scans
- Lack of knowledge of current compliance regulations

Example - Redflag Pentest Report

3. Conclusion

The security assessment of application on the URLs https://sandbox.[redacted] was performed. The pages tested are considered as a representative of the entire application. Consequently, the results must not be taken to be the sum total of the security issues and problems in the application, but as a representative sample.

During this process, [redacted] had found 6 vulnerabilities and upon re-test 1 high and 1 medium severity vulnerabilities were remediated. We highly recommend that low vulnerabilities to be fixed or remediated on production.

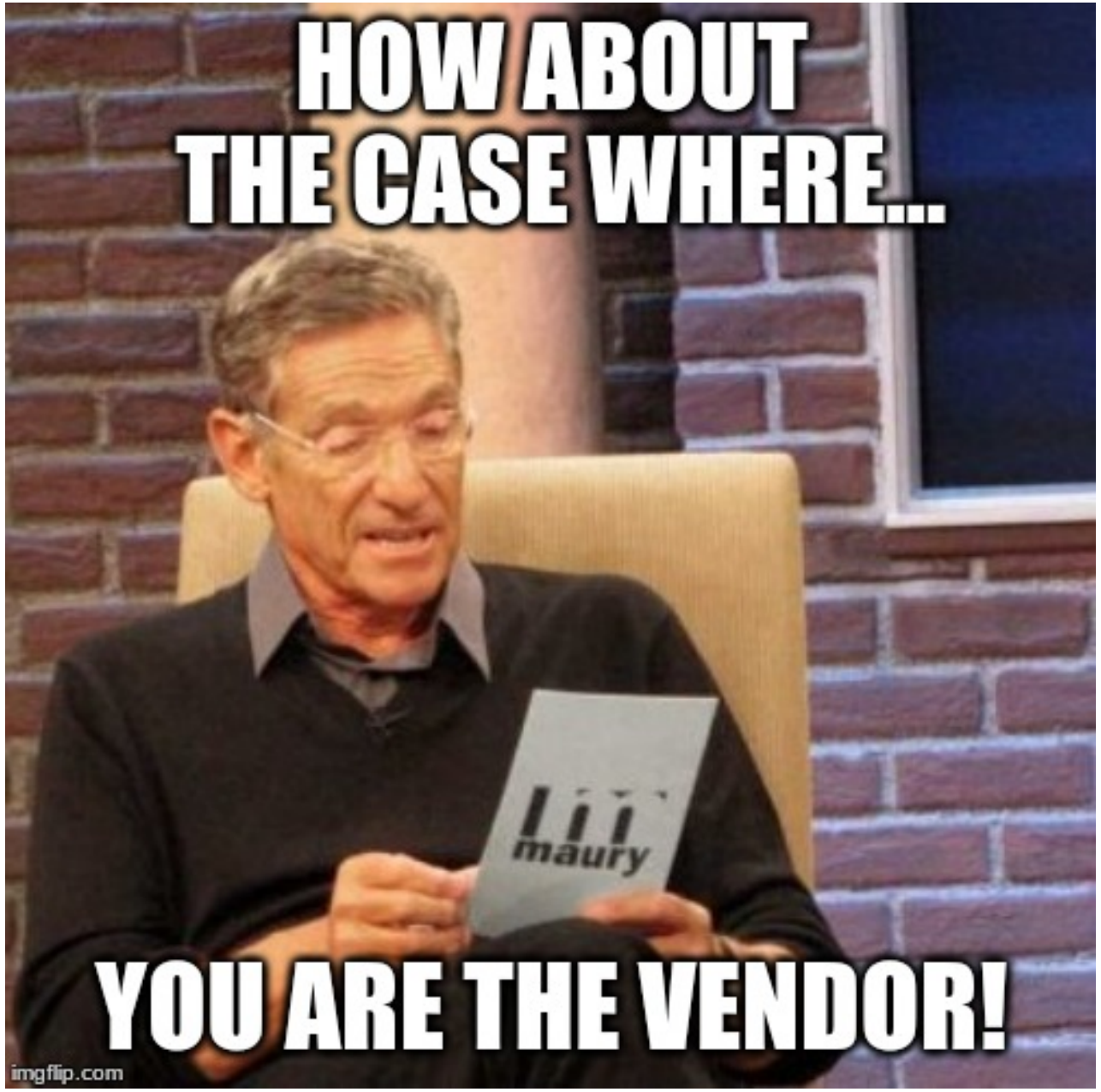
13. COMPANY'S OBLIGATION TO PROVIDE SOURCE CODE.

In the event the source code either has not been escrowed or for any reason cannot readily be obtained from the escrow agent, [redacted] shall have the right to obtain source code directly from Company if bankruptcy, receivership, insolvency, reorganization, dissolution, liquidation or similar proceedings

[redacted]

Advanced notice clauses

10.3. Service Provider shall provide reasonable advanced notification, which shall be defined as at least three weeks, to Customer where Service Provider wishes to engage a Subprocessor to process Customer Data and shall provide, upon Customer's request, the identity and location of the Subprocessor and a description of the processing to be subcontracted or outsourced to such Subprocessor.


HOW ABOUT
THE CASE WHERE...
maury
YOU ARE THE VENDOR!
imgflip.com

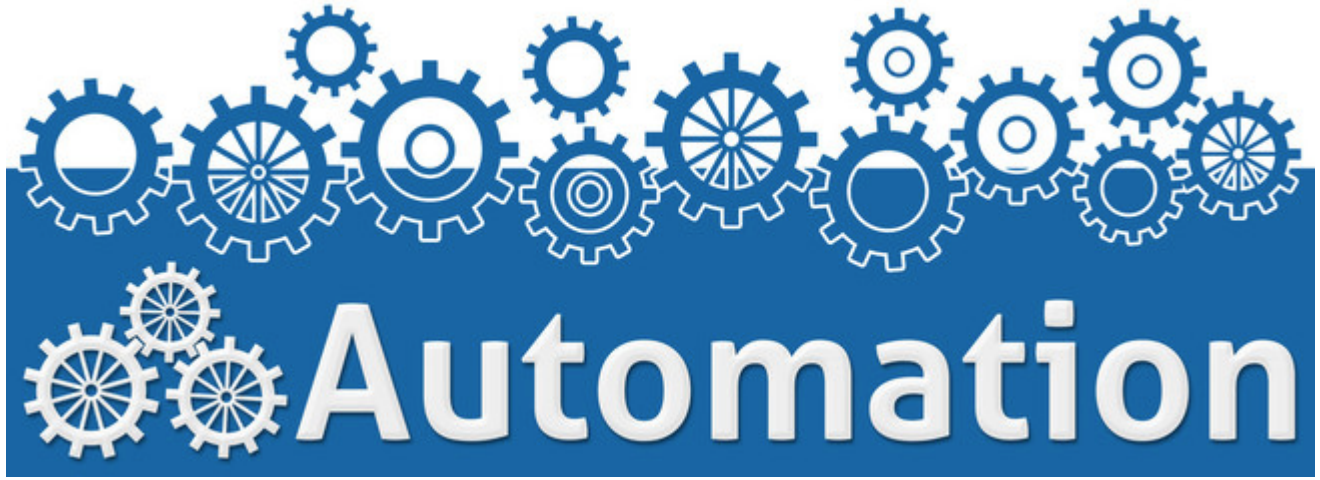
Be prepared!

- Be ready with acceptable contracts (DPA's, MSA's)
- Due diligence package
- Most recent vulnerability scan, SOC 2 report, penetration tests, trusted advisor reports etc..
- Completed questionnaires (CAIQ, SIG, HECVAT)

How to keep up with all of this

- Spreadsheets and file storage

- Procurement departments
- Vendor risk applications

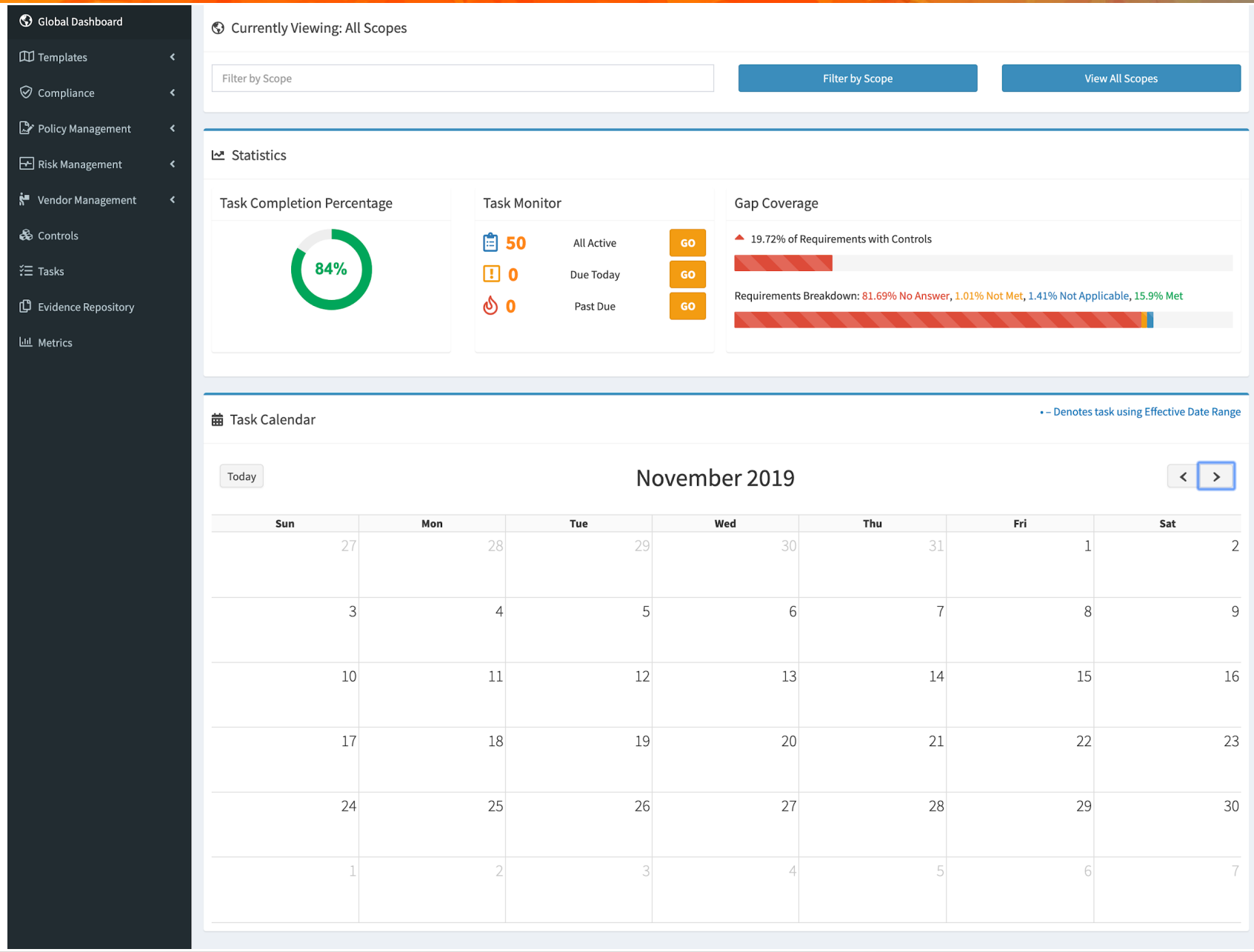


Source blog.kizian.com

KCM GRC Vendor Risk

- This is what we use internally

- Part of KnowBe4 KCM GRC Product


Global Dashboard
Templates
Compliance
Policy Management
Risk Management
Vendor Management
Controls
Tasks
Evidence Repository
Metrics
Currently Viewing: All Scopes
Filter by Scope
Filter by Scope
View All Scopes
Statistics
Task Completion Percentage
84%
Task Monitor
50
All Active
GO
0
Due Today
GO
0
Past Due
GO
Gap Coverage
19.72% of Requirements with Controls
Requirements Breakdown: 81.69% No Answer, 1.01% Not Met, 1.41% Not Applicable, 15.9% Met
Task Calendar
• – Denotes task using Effective Date Range
Today
November 2019
Sun
Mon
Tue
Wed
Thu
Fri
Sat
27 28 29 30 31 1 2
3 4 5 6 7 8 9
10 11 12 13 14 15 16
17 18 19 20 21 22 23
24 25 26 27 28 29 30
1 2 3 4 5 6 7

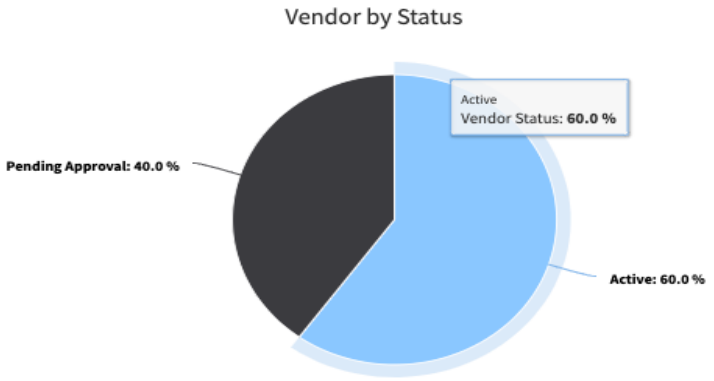
KnowBe4

Vendor Status

Search by Status...

Name	Contact Email	Status
Logistics Management Organization		Active
Supply Chain Distribution		Pending Approval
Accounting Services		Pending Approval
Customer Management Service Provider, Inc.		Active
		Active

5 records

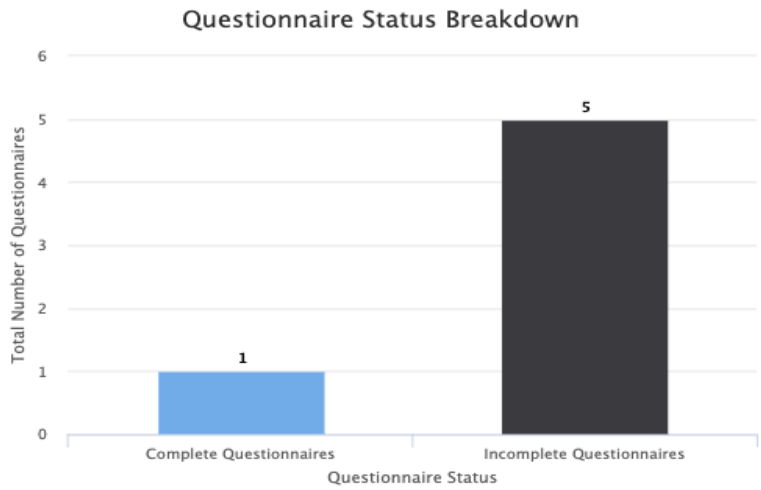


Outstanding Vendor Questionnaires

Search Questionnaires...

Vendor Name	Questionnaire	Status
Supply Chain Distribution	External Vendor Questionnaire	Sent
Accounting Services		Sent
		In Review
Logistics Management Organization	CAIQ Full (2019)	In Review
Customer Management Service Provider, Inc.	CAIQ Full (2019)	Sent

5 records



Thank You!

Brian Jack, CISO, DPO and
Lecio de paula, Data Privacy Director

KnowBe4