John Reeman

CEO & Founder – Cyooda Security

The Hamster Wheel of Death

“Learnings from navigating third party audits over the last 10 years!”

About Me

- 30 years in cyber security
- Software engineer by trade
- Experienced building security programs from the ground up or fixing ones that are broken!
- DFIR
- Threat Hunting
- Generative AI and RAG

A brief history of standards and auditing

1972: NIST was born

JUNE 1974: 1st guideline on IT Physical Security and Risk Management

ARPIL 1988: NIST publish a guide to ”Auditing for controls and security”

FEB 1995: BS7799 Code of practice for Information Security (origins from Royal Dutch/Shell)

FEB 2005: NIST Publication 800-53 “Recommended Security Controls for Federal Information Systems”

OCT 2005: ISO27001 First published (Originated from BS7799) – International standard to manage Information Security

OCT 2005: ISO27002 First Published – Guideline on information security controls

APR 2010: SOC 1, SOC 2 and SOC 3 announced (Part of SSAE 16) to replace SAS 70

Third Party Audit Industry $$$ Value

USD $7.42b in 2023

Growing at a rate of 15%

Forecast in 2030 USD $20b

The Magic Q and Who's Who in the Zoo…

The Pick ‘N’ Mix of Standards…

ISO 27001

NIST

COBIT

ISO27002

PCI-DSS

FISMA

HIPPA

CIS

SOX

GLBA

GDPR

CSA

Welcome to Excel Hell…

C12 | Do you ensure that all default passwords and usernames for all components in the environment used to provide services to us are reset, up

	A	B	C	D	E
1			Question	Main Response	Fur
2	Security Domain	ID	Description	Response	Further Guidance	Evidence (cor
3	General	GE-01	Are the services that your organisation provides located in Australia?		If you answered 'No' then please specify where your services are located and if in multiple locations please list them.	
4		GE-02	Do you provide consultancy services?		If so please describe the safeguards you have in place to protect <COMPANY NAME> data whilst in the possession of your consultants.	
5		GE-03	Is your solution or service an on premises service or a cloud solution (SaaS, PaaS, IaaS)?		If a cloud solution please provide a brief description of the provider (e.g. AWS, Azure, Google etc) and state whether you operate a multi-tenant or single tenant solution.	
6	Identity and Access Management	IAM-01	Do you attribute all user accounts to an individual user identity?		Please describe what technology is used to manage these accounts. Are these accounts managed centrally?	
7		IAM-02	Do you utilise shared accounts in the services that you provide?			
8		IAM-03	Is Federated login supported for the services that you provide?		Does your solution support Single Sign-on with Identity providers such as okta, Google, Microsoft Azure?	
9		IAM-04	Do you require users to authenticate with a loginID and password as a minimum?		Please describe the details of the password policy. Please provide the following details: - Password complexity - Password length - Password History - Password Expiry - Password reset (account lockout after n failed attempts)	
10		IAM-05	Do you require the use of MFA for all privileged actions in the environment?			
11		IAM-06	Do you enforce the principal of least privilege in the environment used to provide services?		Please describe what security controls are in place to achieve this.	
12		IAM-07	Do you ensure that all default passwords and usernames for all components in the environment used to provide services to us are reset, updated or disabled?			

START HERE | ORG Details | TPRA | +

How many tabs and questions?

30 + Tabs

700+ Questions

The Hamster Wheel of Perpetual Audits

Don’t talk to me about Portals!

So, remember this lot…

They reckon they save you this…

But the reality is this…

How much time? – WTF!

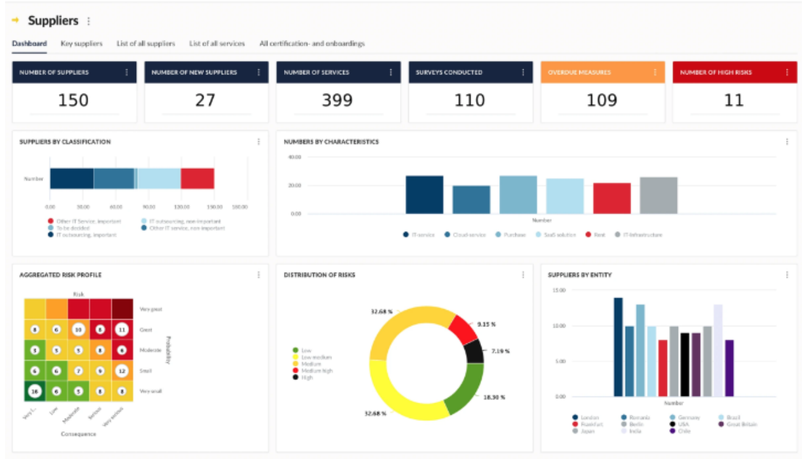
25 Hours a week

Question format timeline....

10 Years ago

Security Domain	ID	Question	Main Responses		Further Information Requir
		Description	Response	Further Guidance	Evidence (commentary, documents,
General	GE-01	Are the services that your organisation provides located in Australia?		If you answered 'No' then please specify where your services are located and if in multiple locations please list them.	
	GE-02	Do you provide consultancy services?		If so please describe the safeguards you have in place to protect <COMPANY NAME> data whilst in the possession of your consultants.	
	GE-03	Is your solution or service an on premises service or a cloud solution (SaaS, PaaS, IaaS)?		If a cloud solution please provide a brief description of the provider (e.g. AWS, Azure, Google etc) and state whether you operate a multi-tenant or single tenant solution.	
Identity and Access Management	IAM-01	Do you attribute all user accounts to an individual user identity?		Please describe what technology is used to manage these accounts. Are these accounts managed centrally?	
	IAM-02	Do you utilise shared accounts in the services that you provide?			
	IAM-03	Is Federated login supported for the services that you provide?		Does your solution support Single Sign-on with Identity providers such as okta, Google, Microsoft Azure?	
	IAM-04	Do you require users to authenticate with a loginID and password as a minimum?		Please describe the details of the password policy. Please provide the following details: - Password complexity - Password length - Password History - Password Expiry - Password reset (account lockout after n failed attempts)	
	IAM-05	Do you require the use of MFA for all privileged actions in the environment?			
	IAM-06	Do you enforce the principal of least privilege in the environment used to provide services?		Please describe what security controls are in place to achieve this.	
	IAM-07	Do you ensure that all default passwords and usernames for all components in the environment used to provide services to us are reset, updated or disabled?			

Now



The Irony of Portals

Operated by….

3rd Party

Artefacts and Certification Proof

Each Audit varies….

Some ask several artefacts
e.g. ISO27K Certs, SOC 2,
Security Policies,
Incident Response Plans

Others want everything but the…

Legal Contracts 3rd, 4th and 5th Parties!

- Clauses in contracts
- Right to Audit
- With the increase in breaches more questions are appearing on 4th and 5th parties

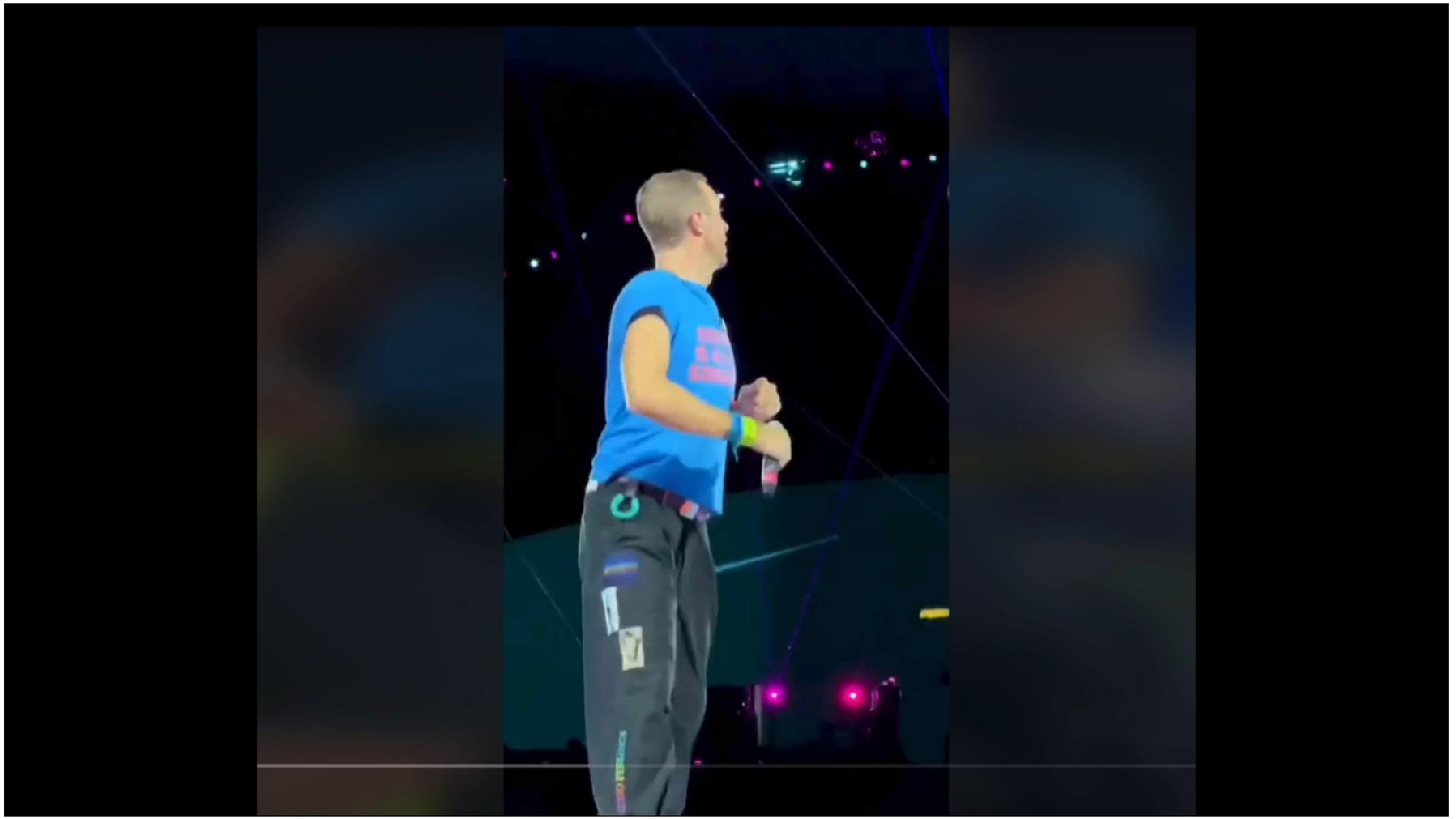
Other Challenges

- Over reliance on point in time audits
- Misalignment of security context, risk tolerance and maturity
- Trend of pushing liability of compliance on to the entity being audited (CPS234)
- Lack of subject matter expertise
- Over resilience of weighting and severity of questions – High risk vs Low risk

Strange questions and funny moments…

Funny questions I’ve been asked…

Security Guards



No Context…

700 + Audits

6 Years

ONLY 1 Organisation asked if the questions were relevant!

What’s helped?

Knowledge bank of answers

Knowledge bank of artefacts

Being consistent

Push back

Certification to some degree

The Industry is broken

What needs to change

Audit Compliance is nothing more than a…

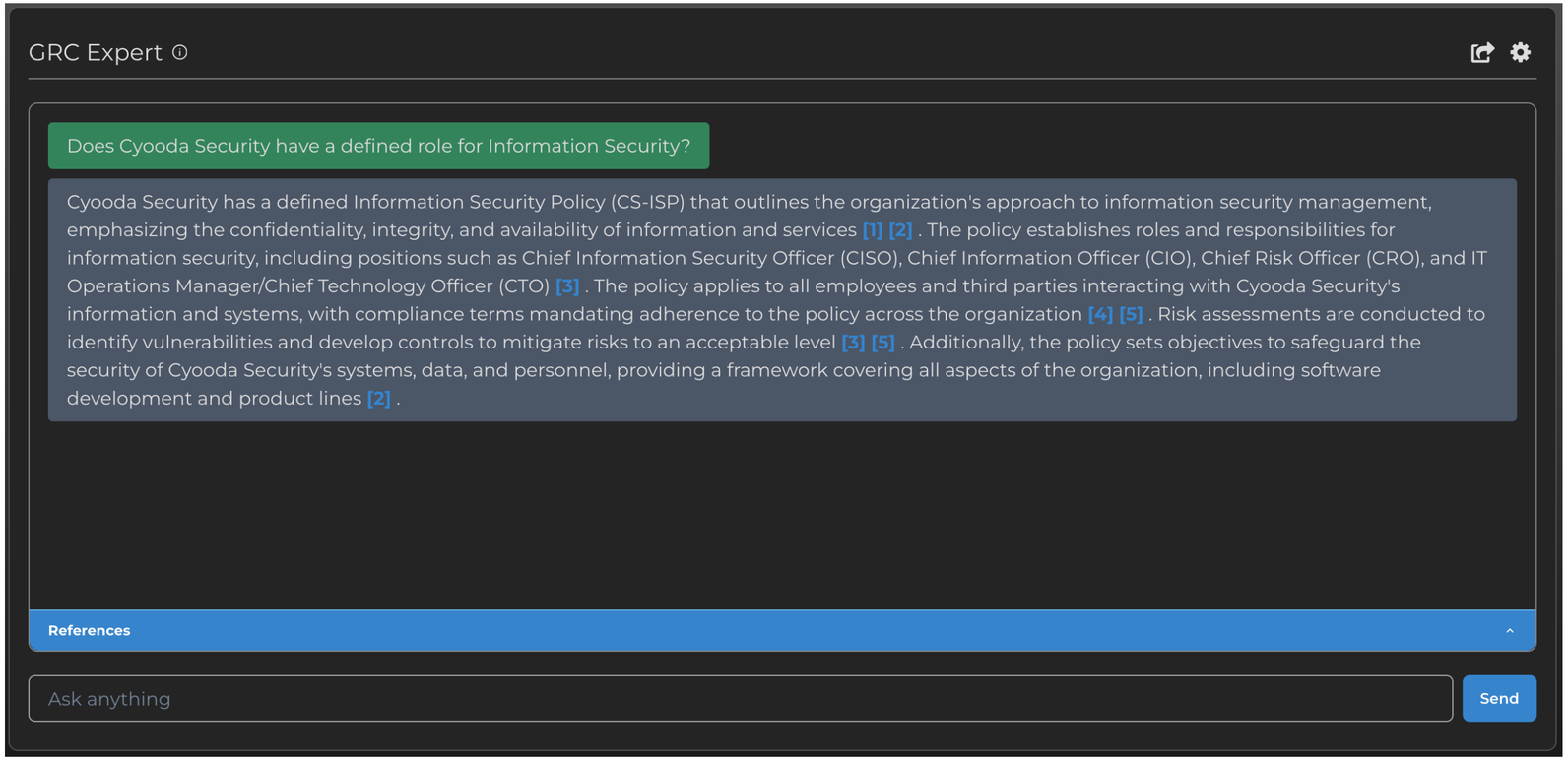
But we are far from SECURE

A glimpse into the future with AI

Retrieval Augmentation Generation (RAG)

Natural Language Processing (NLP)

Generative AI



Contact

John Reeman
john@cyooda.com