Instrument flight rules

Navigating Cyber Security in a Cloud Landscape

Richard Miller


Max cont.
SVS-1
CHECK LIST
TAKE OFF
AIRSPEED
DAYTRON
ASPEN AVIONICS
EVOLUTION
AUTOPILOT


TEMP°C
30+0-30
PRESS ALT
200
180
160
140
120
100
80
60
40
AIRSPEED
KNOTS
TAS
VACUUM
ALTIMETER
CALIBRATED TO 20,000FT
D.C. ELEC.
TURN COORDINATOR
L
R
2 MIN.
NO PITCH INFORMATION
N
W
E
VERTICAL SPEED
UP
DN
100 FEET PER MIN

Cloud Security Challenges

Challenge #1

The perimeter is ~~dead~~ changing

01010100 01101000 01100101 00100000 01110000
01100101 01110010 01101001 011011[illegible]101
01110100 01100101 01110010 001000[illegible]001
01110011 00100000 01100100 0110010[illegible]0001
01100100

011

01000011 01110010
01101111 01110111
01101110 00100000
01101010 01100101
01110111 01100101
01101100 01110011

Identity perimeter

Network perimeter


In Loving Memory Of
PHILLIP RYAN.
WHO DIED 10TH OCTOBER 1907,
AGED 70 YEARS.
Also WILLIAM RYAN.
DIED 14TH MAY 1907, AGED 23 YEARS.
Also DENIS RYAN.
DIED 20TH JUNE 1928, AGED 34 YEARS
Also PHILLIP BARNEY RYAN
BETTY MARGARET RYAN


VPN

Challenge #2

People

Challenge #3

Shadow IT


Trello


Dropbox


slack


mailchimp


box


qualtrics


Google


zoom


amazon
web services


Linked in

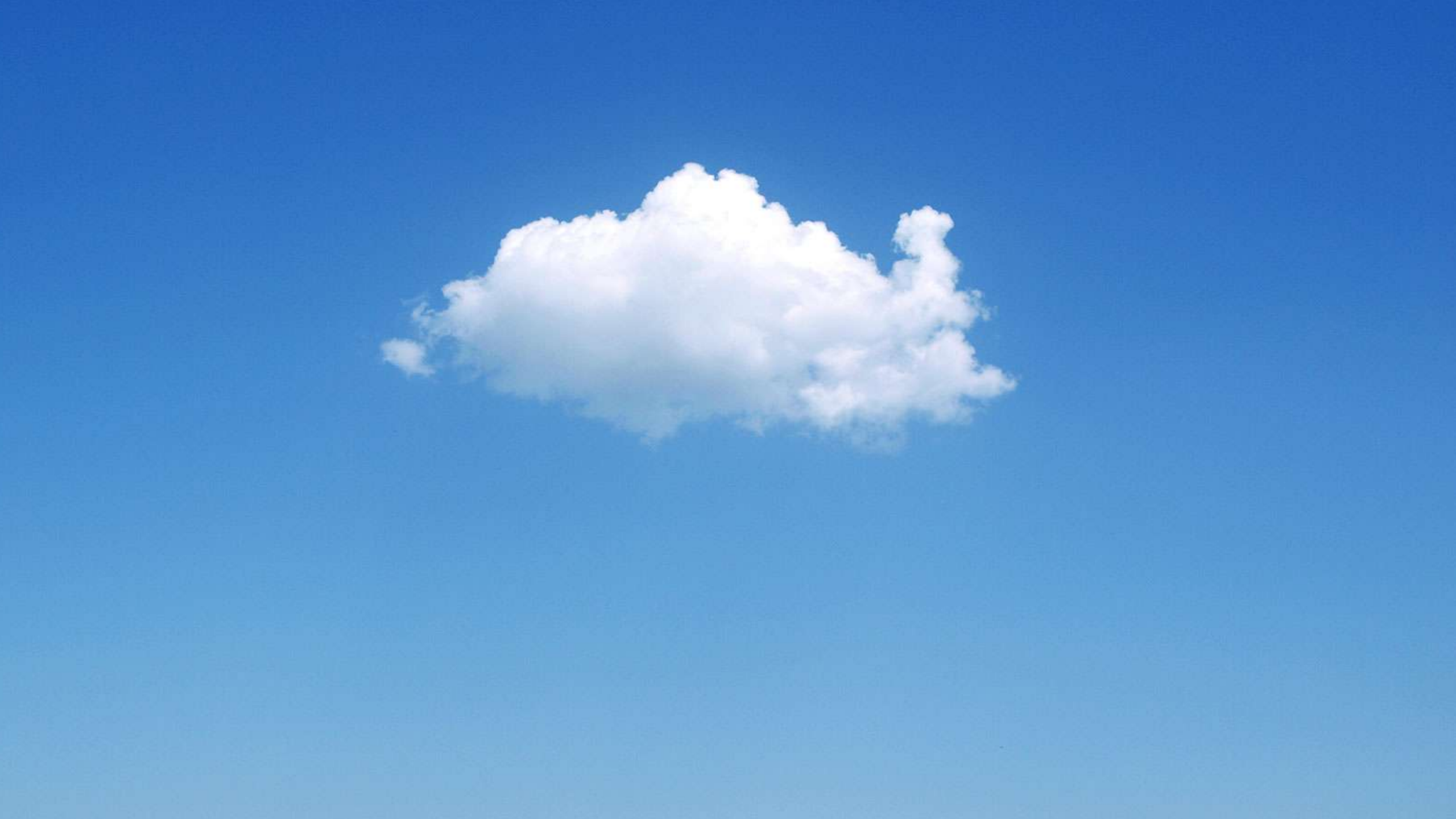

GitHub


Jira
Confluence
Bitbucket


in VISION

Challenge #4

Where is my data?



Challenge #5

3rd party complacency

Your cloud providers all have sophisticated certification and compliance programs

Shared Responsibility Model

	On Prem	IaaS	PaaS	SaaS
Governance, Risk, Compliance	✓	✓	✓	✓
Data Security	✓	✓	✓	✓
Client Endpoints	✓	✓	✓	✓
Identity & Access Management	✓	✓	✓X	✓X
Application Security	✓	✓	✓X	X
Operating System	✓	✓	X	X
Hypervisor Security	✓	X	X	X
Storage	✓	X	X	X
Host Security	✓	X	X	X
Infrastructure Security	✓	X	X	X
Physical Security	✓	X	X	X

✓ You X Cloud provider

WHO IS RESPONSIBLE?

YOU ARE

The challenges

1. The perimeter
2. People
3. Shadow IT
4. Where is my data?
5. 3rd party complacency

The fundamentals

"He who defends everything defends nothing"

Frederick the Great

The fundamentals

1. Understand your risk appetite
2. Identify your crown jewels
3. Proportional defense

Tip #1

Define an Information Security Framework and Roadmap

Tip #2

Get buy in at the highest levels

Tip #3

Start building out an Information Security Management System

Externally certified ISMS

- Risk-based approach to security compliance, not prescriptive
- Commitment to managing information security risk
- Continual improvement
- Maintain a risk register and prioritise risks
- Externally certified annually

Risk Assessment Matrix					
Risk Impact	Risk Likelihood				
	Rare (1)	Unlikely (2)	Possible (3)	Likely (4)	Almost Certain (5)
Insignificant (1)	Informational (1)	Informational (2)	Informational (3)	Low (4)	Low (5)
Minor (2)	Informational (2)	Low (4)	Low (6)	Medium (8)	Medium (10)
Moderate (3)	Informational (3)	Low (6)	Medium (9)	High (12)	High (15)
Major (4)	Low (4)	Medium (8)	High (12)	High (16)	Critical (20)
Extreme (5)	Low (5)	Medium (10)	High (15)	Critical (20)	Critical (25)

Assess impact across

- Financial impact
- Business interruption
- Reputation
- Information Security Objectives

Determine course of action based upon risk

Tip #4

Trust no one

Tip #5

Create a cyber aware culture

Tip #6

Run regular phishing simulations

Tip #7

Enable MFA everywhere

Tip #8

Enable SSO everywhere

Tip #9

Nextgen antivirus

Tip #10

Lock down USB

Tip #11

Web application firewall

Top Tip #12

Cloud Access Security Brokers (CASB)

Tip #13

Regular penetration tests

Tip #14

Secure code training

OWASP Top 10 - 2013		OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Source: https://www.owasp.org

Tip #15

Not using SSL - seriously?
security headers
cookies

Tip #16

3rd party contracts

Final tip 😄

Solid incident response plan

Be aware ...

Notifiable Data Breaches Scheme

Thank you