ARMOR | Pulsant | SECURECON 2019 | DALLAS, TEXAS

PULSANT SHARES BEST PRACTICES:

IMPROVING YOUR SECURITY POSTURE IN A HYBRID CLOUD ENVIRONMENT

ROBIN FERRIS
Cloud Solutions Architect
@stratusCub

AGENDA

1. Introduction
2. Where Have We Come From?
3. Mindset – It's The Same But Different
4. Examples
5. Takeaways & Wrap-Up

ARMOR. MAKING CLOUD SECURITY SIMPLE
I want to learn more about
SECURITY-AS-A-SERVICE
SECURE HOSTING

ROBIN FERRIS

Solution Architect

Robin has over 20 years of experience working in IT, with extensive experience in cloud, migration and hosting. Robin began his career in desktops and application repackaging, before moving into server-side software, and then into platforms-as-a-service (PaaS) and cloud.

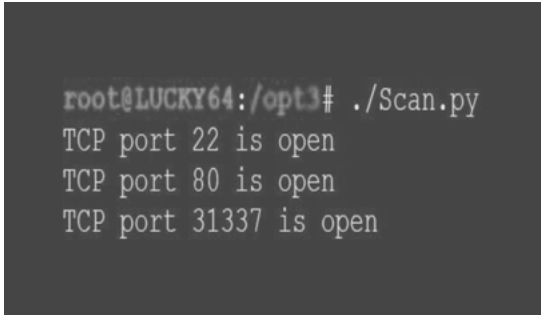
Robin deals with the cloud journey and hybrid question on a daily basis, and spends his time focusing on Azure, Azure Stack and security as a whole.

Contact me at:
robin.ferris@pulsant.com
@stratusCub

WHAT OPERATING SYSTEM ARE YOU?

WHERE HAVE WE COME FROM?

WHERE HAVE WE COME FROM?



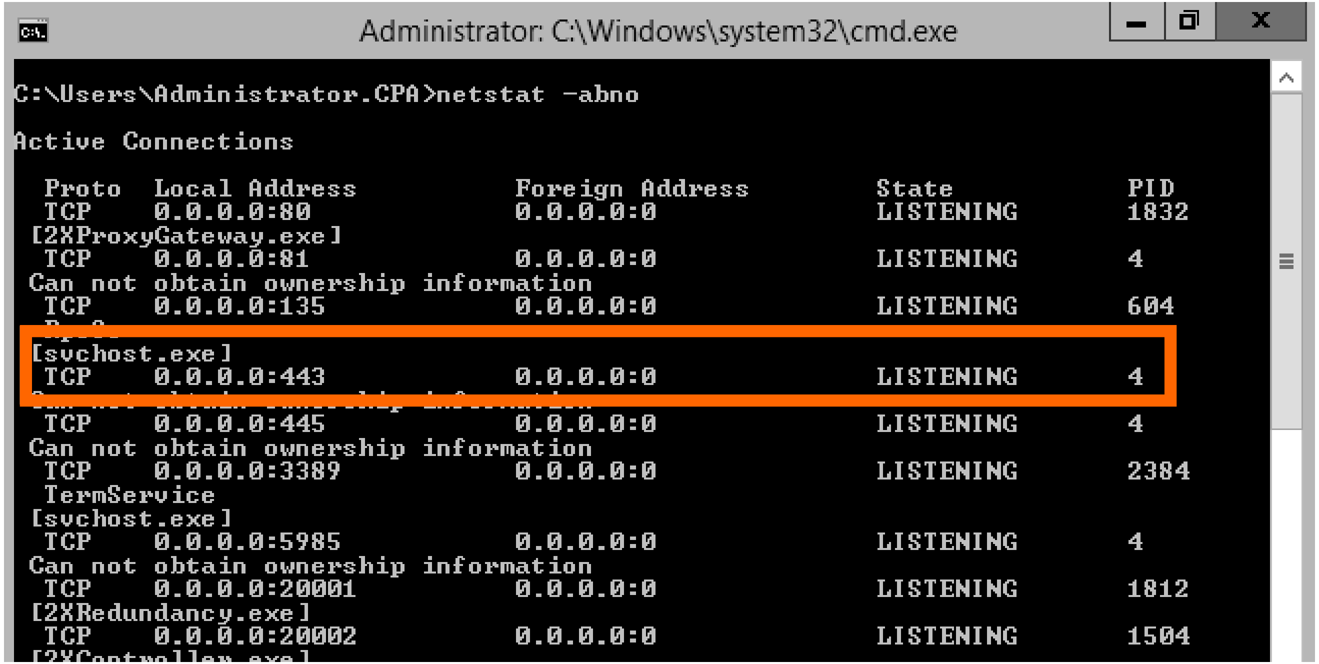
```
root@LUCKY64:/opt3# ./Scan.py
TCP port 22 is open
TCP port 80 is open
TCP port 31337 is open
```

```
 _   _
((___))
[ x x ]
 \   /
 (' ')
  (U)
```

WHAT ARE WE PROTECTING OUR ENVIRONMENTS AND DATA FROM?

REMOTELY EXPLOITABLE VULNERABILITIES **and one other thing …..**

WHAT ARE WE PROTECTING OUR ENVIRONMENTS AND DATA FROM?

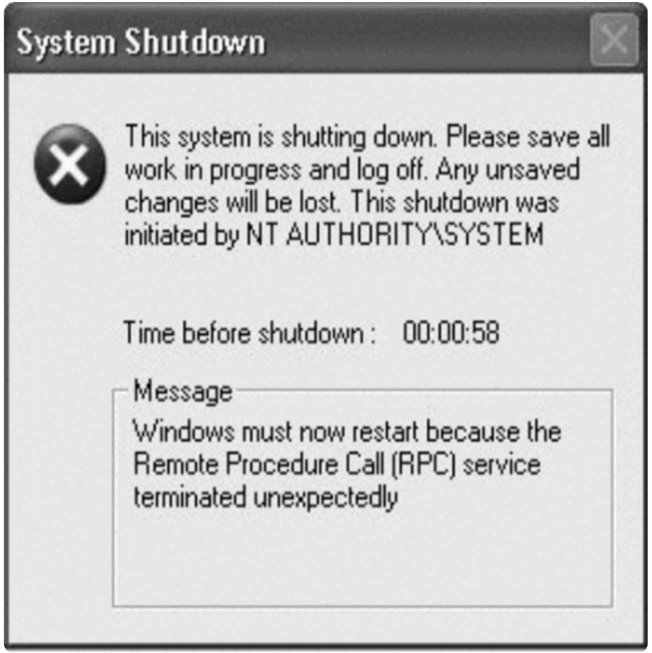


```
C:\Users\Administrator.CPA>netstat -abno

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       1832
 [2XProxyGateway.exe]
  TCP    0.0.0.0:81             0.0.0.0:0              LISTENING       4
 Can not obtain ownership information
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       604
  RpcSs
 [svchost.exe]
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING       4
 Can not obtain ownership information
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
 Can not obtain ownership information
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       2384
  TermService
 [svchost.exe]
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING       4
 Can not obtain ownership information
  TCP    0.0.0.0:20001          0.0.0.0:0              LISTENING       1812
 [2XRedundancy.exe]
  TCP    0.0.0.0:20002          0.0.0.0:0              LISTENING       1504
 [2XController.exe]
```

2003



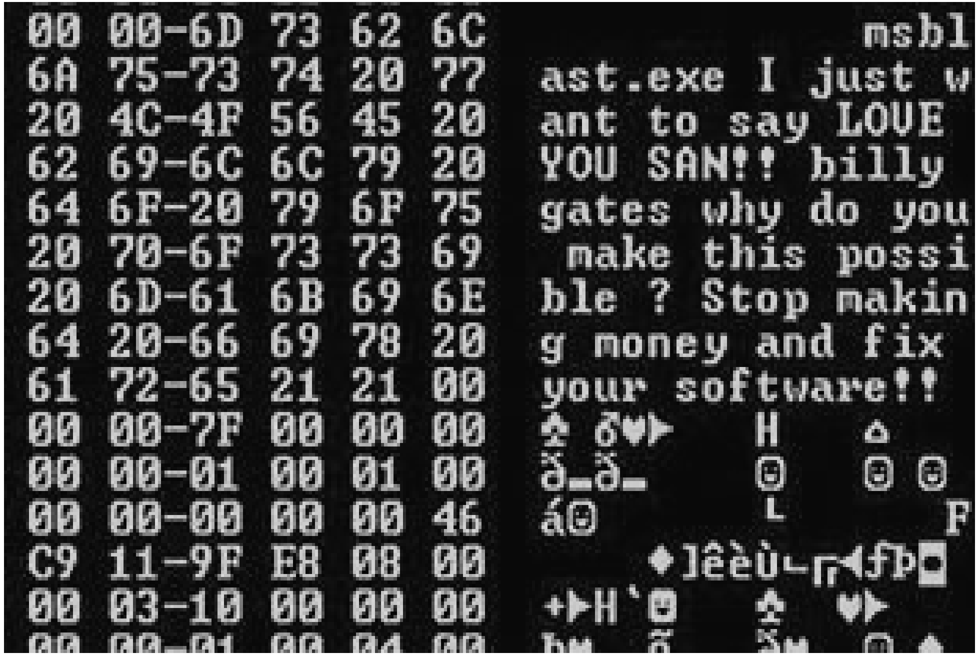
System Shutdown

This system is shutting down. Please save all work in progress and log off. Any unsaved changes will be lost. This shutdown was initiated by NT AUTHORITY\SYSTEM

Time before shutdown : 00:00:58

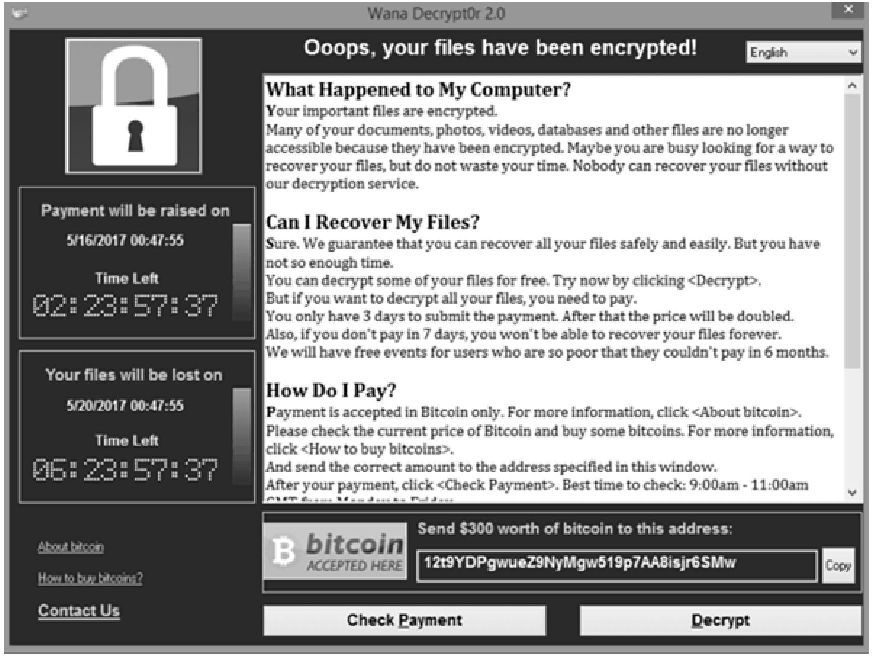
Message

Windows must now restart because the Remote Procedure Call (RPC) service terminated unexpectedly



```
00 00-6D 73 62 6C      msbl
6A 75-73 74 20 77  ast.exe I just w
20 4C-4F 56 45 20  ant to say LOVE
62 69-6C 6C 79 20  YOU SAN!! billy
64 6F-20 79 6F 75  gates why do you
20 70-6F 73 73 69   make this possi
20 6D-61 6B 69 6E  ble ? Stop makin
64 20-66 69 78 20  g money and fix
61 72-65 21 21 00  your software!!
00 00-7F 00 00 00  ♠ ō♥▶    H   ⌂
00 00-01 00 01 00  ð_ð_     ☺   ☺ ☺
00 00-00 00 00 46  á☺       └      F
C9 11-9F E8 08 00     ♦Jêèù└╓◄ƒÞ■
00 03-10 00 00 00  ♦▶H`☺    ♠  ♥▶
```

2017



Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

HYBRID

WHO IS RUNNING IN A
HYBRID IT ENVIRONMENT NOW?

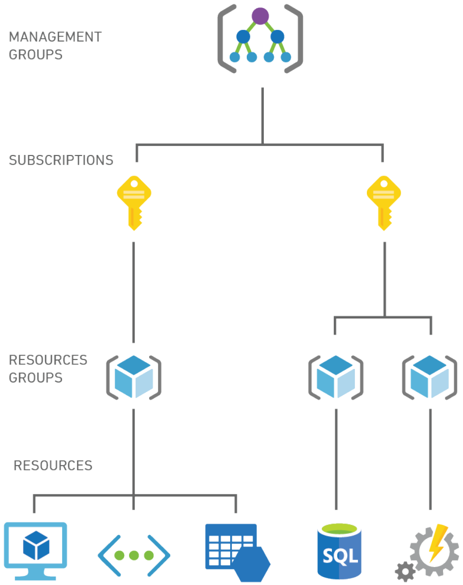
> The Cloud is just
> someone else's computer.

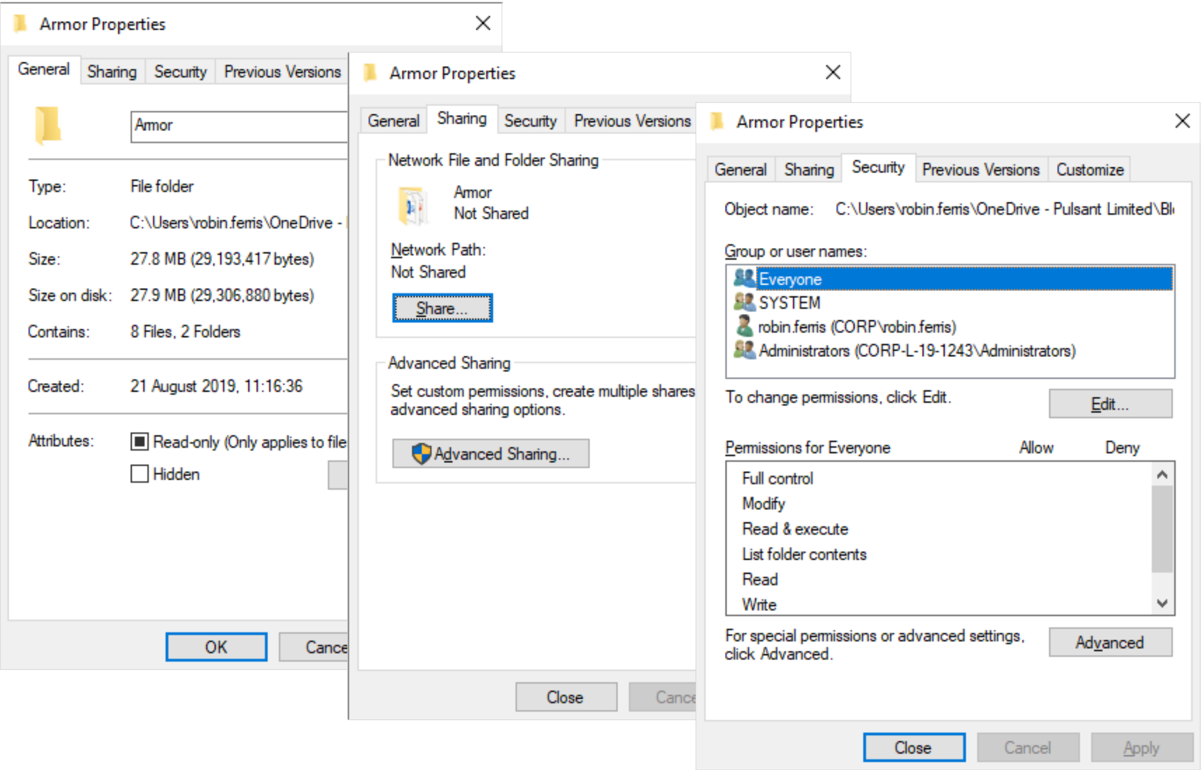
WHAT IS CHANGING WITH HYBRID CLOUD?

Cleaning up setups • Going well beyond IaaS

MINDSET – IT’S THE SAME BUT DIFFERENT

MINDSET – IT'S THE SAME BUT DIFFERENT





Armor Properties

Armor

Type: File folder

Location: C:\Users\robin.ferris\OneDrive -

Size: 27.8 MB (29,193,417 bytes)

Size on disk: 27.9 MB (29,306,880 bytes)

Contains: 8 Files, 2 Folders

Created: 21 August 2019, 11:16:36

Attributes: ☒ Read-only (Only applies to file

☐ Hidden

Armor Properties

Network File and Folder Sharing

Armor
Not Shared

Network Path:
Not Shared

Advanced Sharing

Set custom permissions, create multiple shares advanced sharing options.

Armor Properties

Object name: C:\Users\robin.ferris\OneDrive - Pulsant Limited\Bl

Group or user names:

- Everyone
- SYSTEM
- robin.ferris (CORP\robin.ferris)
- Administrators (CORP-L-19-1243\Administrators)

To change permissions, click Edit.

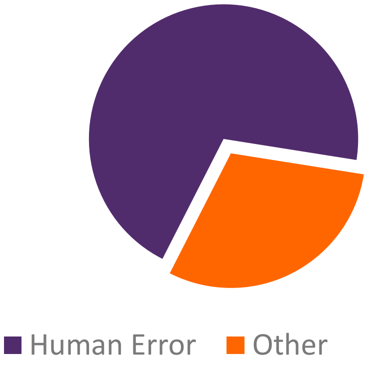
Permissions for Everyone	Allow	Deny
Full control		
Modify		
Read & execute		
List folder contents		
Read		
Write		

For special permissions or advanced settings, click Advanced.

EXAMPLES

HUMAN ERROR

REMOVE THE CHANCE FOR HUMAN ERROR



accenture

DOW JONES

verizon

PASSWORDS

PASSWORDS ARE DEAD!

';--have I been pwned?

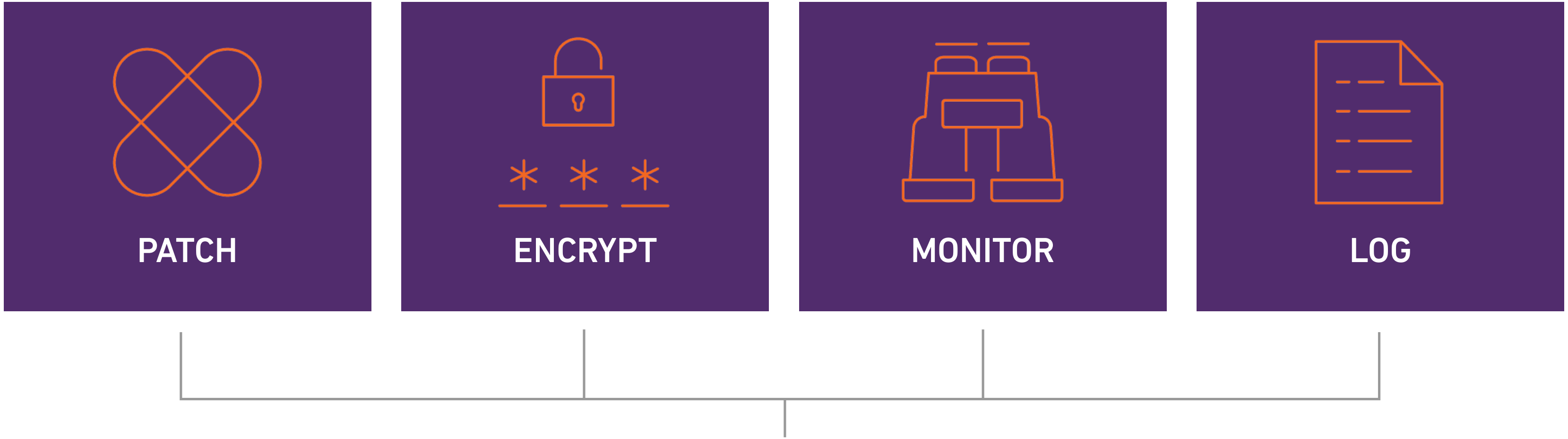
408
pwned websites

8,506,873,299
pwned accounts

102,441
pastes

122,480,433
paste accounts

DO THE BASICS



PATCH

ENCRYPT

MONITOR

LOG

...at Machine Speed!

THINK LIKE YOUR OPPONENT

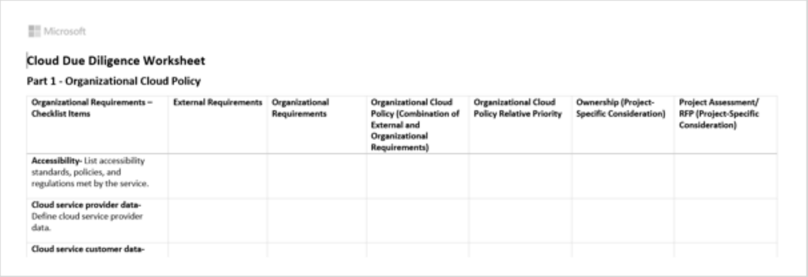
BE THE HACKER

WHAT WOULD THEY BE LOOKING FOR?

ISO/IEC 19086-1:2016

> ....seeks to establish a set of common cloud SLA building blocks (concepts, terms, definitions, contexts) that can be used to create cloud Service Level Agreements (SLAs)

> is for the benefit and use of both cloud service providers and cloud service customers. The aim is to avoid confusion and facilitate a common understanding between cloud service providers and cloud service customers.

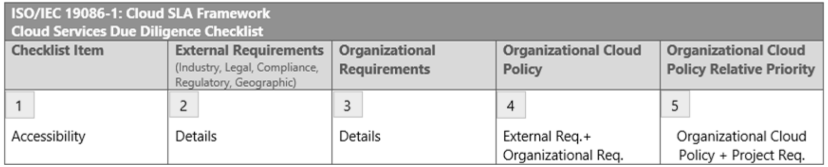


Microsoft

Cloud Due Diligence Worksheet

Part 1 - Organizational Cloud Policy

Organizational Requirements – Checklist Items	External Requirements	Organizational Requirements	Organizational Cloud Policy (Combination of External and Organizational Requirements)	Organizational Cloud Policy Relative Priority	Ownership (Project-Specific Consideration)	Project Assessment/ RFP (Project-Specific Consideration)
Accessibility- List accessibility standards, policies, and regulations met by the service.						
Cloud service provider data- Define cloud service provider data.						
Cloud service customer data-						



ISO/IEC 19086-1: Cloud SLA Framework

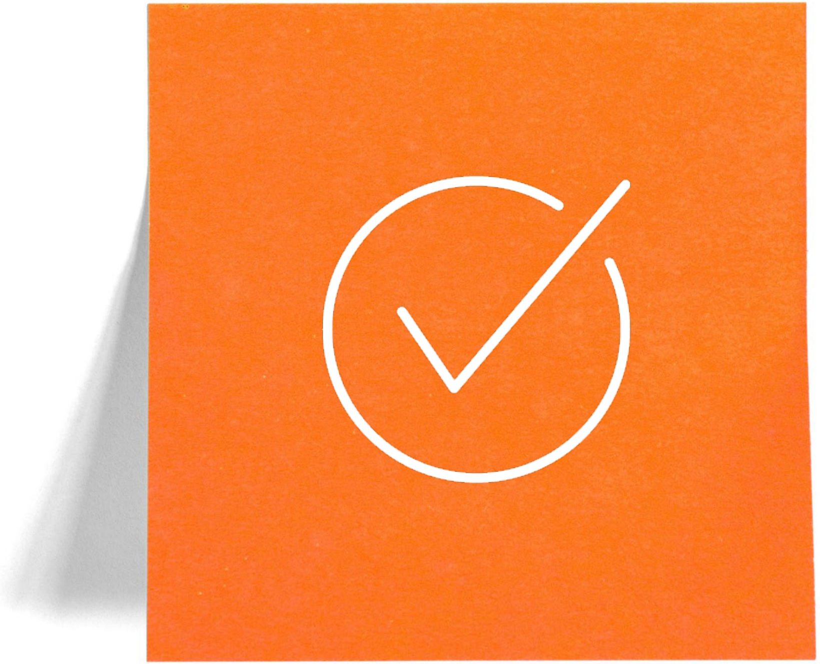
Cloud Services Due Diligence Checklist

Checklist Item	External Requirements (Industry, Legal, Compliance, Regulatory, Geographic)	Organizational Requirements	Organizational Cloud Policy	Organizational Cloud Policy Relative Priority
1	2	3	4	5
Accessibility	Details	Details	External Req.+ Organizational Req.	Organizational Cloud Policy + Project Req.

ISO/IEC 19086-1:2016

GOVERNANCE & COMPLIANCE:

- AU Protected
- FedRAMP
- FFIEC
- HIPAA/HITRUST
- NIST SP 800-171
- PCI DSS
- UK NHS
- UK OFFICIAL
  - □ IaaS web application
  - □ PaaS web application



TAKEAWAYS AND WRAP-UP

TAKEAWAYS – BEST PRACTICES

1. Simplify it, draw parallels with existing processes.
2. Remove the chance for Human Error.
3. Passwords are dead – 2FA FTW.

TAKEAWAYS – BEST PRACTICES

4. Do the basics – patch, encrypt, monitor, and log
5. Think like your opponent.
6. ISO/IEC 19086-1:2016.

Q & A

ROBIN FERRIS - @stratusCub

Cloud Solutions Architect

THANK YOU.

WWW.ARMOR.COM

WWW.PULSANT.COM