Digital Resilience and High Availability

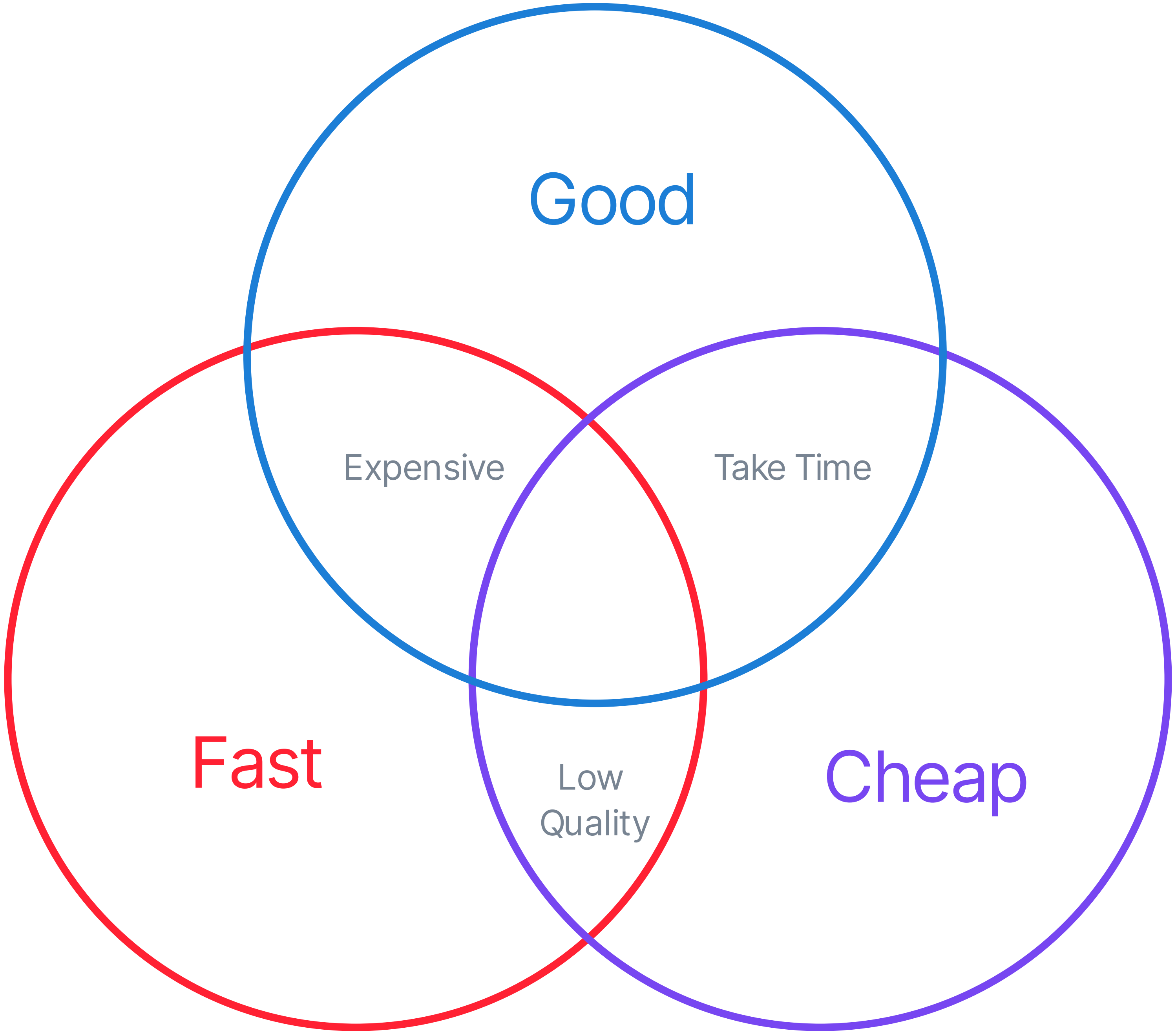
by BlueT M. Lien

ⓘ BlueT / Matthew Lien - 練喆明

國家資通安全研究院 - 韌性架構總顧問

About...

Hello World



Good

Expensive

Take Time

Fast

Low Quality

Cheap

Hello World and Go Deeper

朋友們，你們準備好了嗎

!(political correctness)

Content

Digital Resilience and High Availability

And...

regulatory
sast
important
maintainability
personnel
measures
systems
cyclonedx
verified
management
response
prevention
services
data
risk
security
nist
importance
one
model
etc
ref
user
requirements
network
maintaining
vs
resilience
verifiers
missing
concept
assess
infrastructure
role
components
contains
operations
need
online
recovery
areas
cia
discuss
change
focuses
incorporate
explain
high
digital
world
memorized
continuity
docker
plan
physical
flexible
backup
hello
ensure
improve
password
business
implement
rolling
availability
disaster
secrets
definition
monitoring
dast
plans
pdca
system
software
users
incidents
https
know
automation
service
control
place
redundancy
incident
models
already
cybersecurity
includes
technology
selection
regularly
processes
specific
planning
supports
disruption
evaluation
examples
responsibilities
organization

Digital Resilience Cheatsheet

元素　　方法　　特性　　條件

✓ 流程

態度

起

Intro & Overview

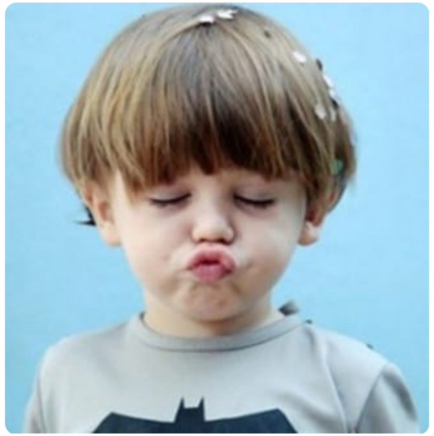
- Definition of digital resilience.
- Why digital resilience is important.

~~Who~~ What is

~~任性~~ 韧性

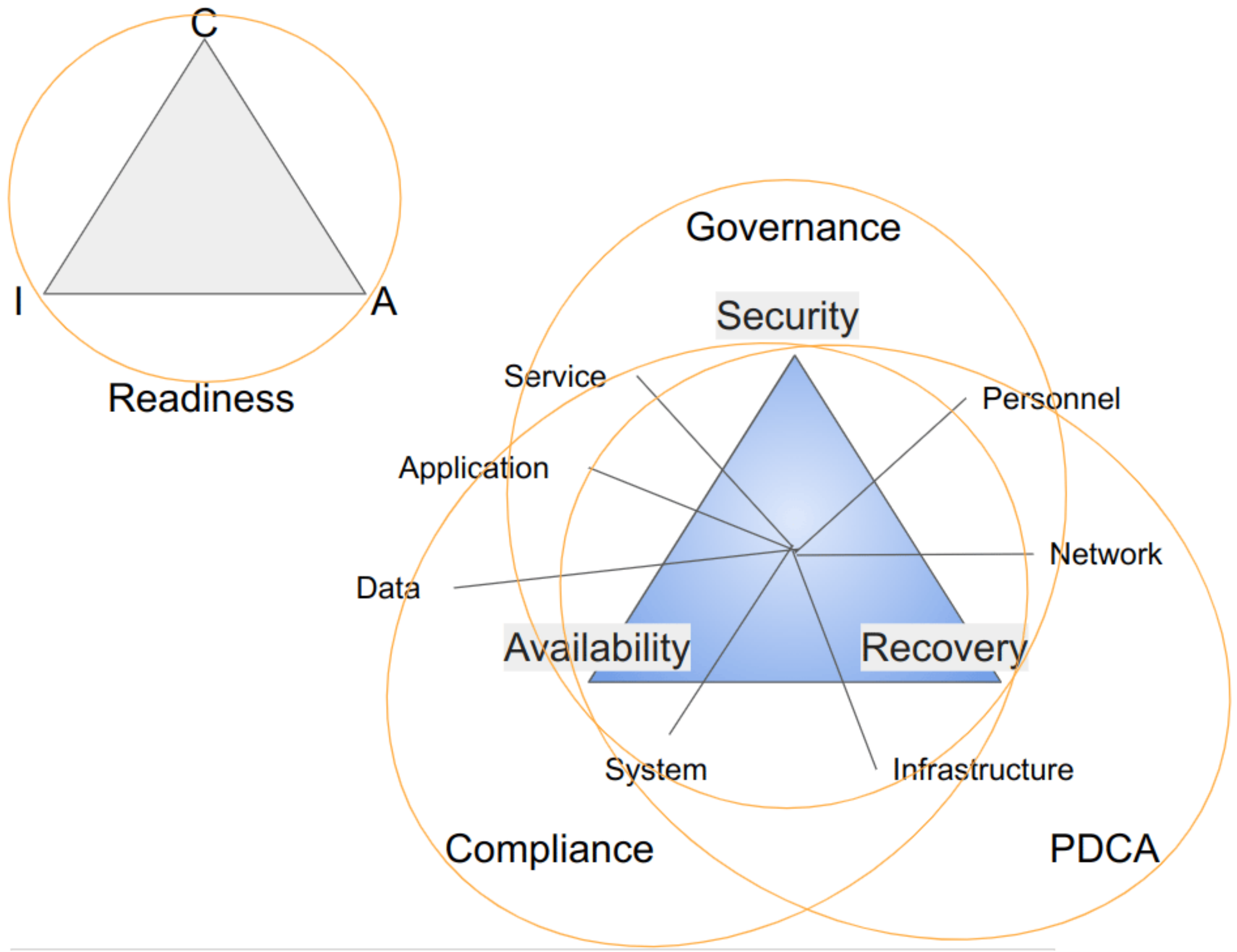
What is

數位~~任性~~韌性



What is

- 難打掛、打不掛、打掛也不怕
- 流程 整個都該是有韌性的
- Proactive, Reactive


C
I
A
Readiness
Governance
Security
Service
Personnel
Application
Network
Data
Availability
Recovery
System
Infrastructure
Compliance
PDCA

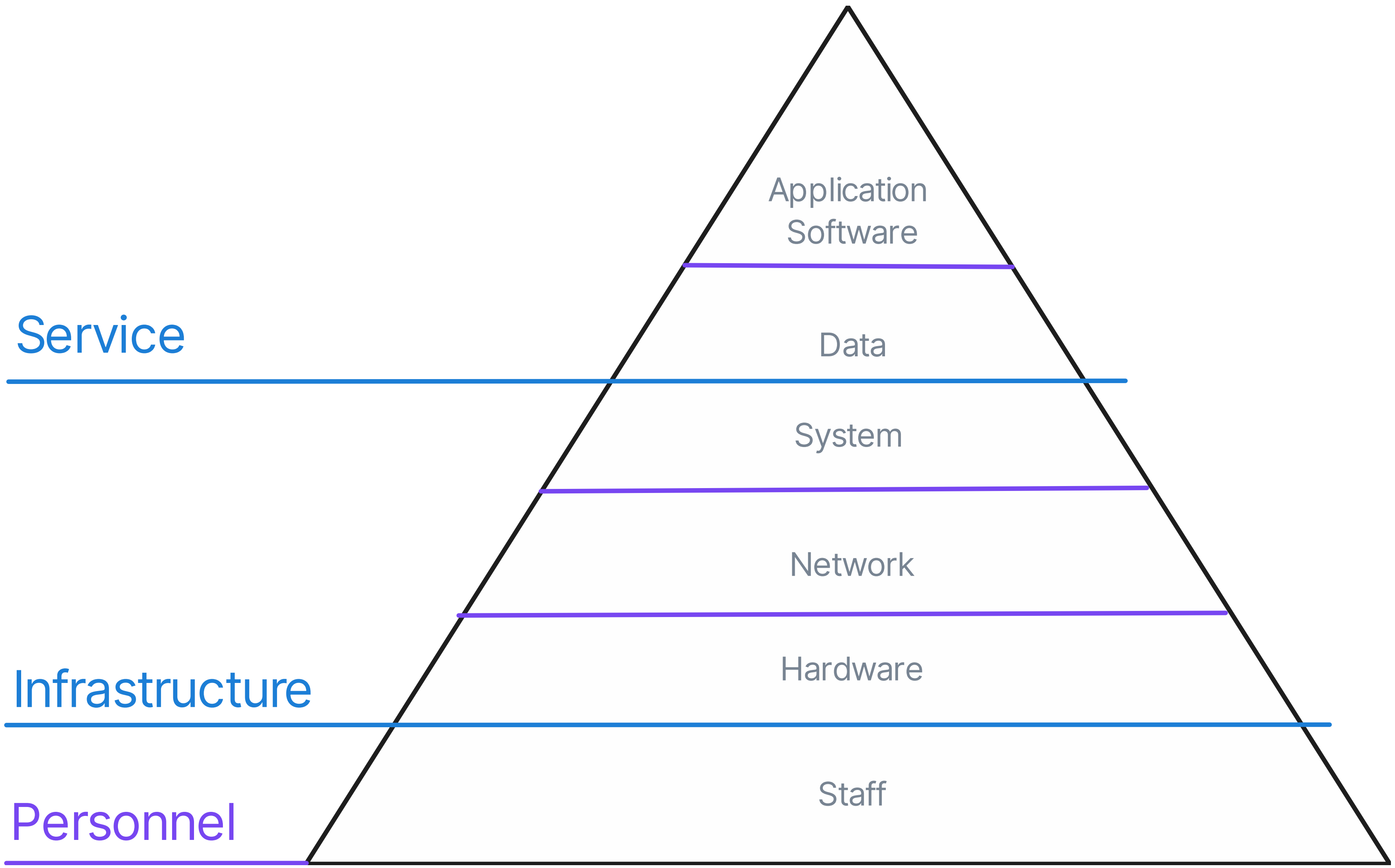
Components

- cybersecurity, high availability, accessibility, maintainability, etc.

Components

整個 流程 都該是有韌性的

- service
- application
- data
- system (online, backup)
- network
- infrastructure
- personnel
- and others (governance, etc)



Service

Infrastructure

Personnel

Application Software

Data

System

Network

Hardware

Staff

Digital Resilience Cheatsheet

- service
- application
- data
- system (online, backup)
- network
- infrastructure
- personnel

Models

NIST, ISO, SDG 9, etc

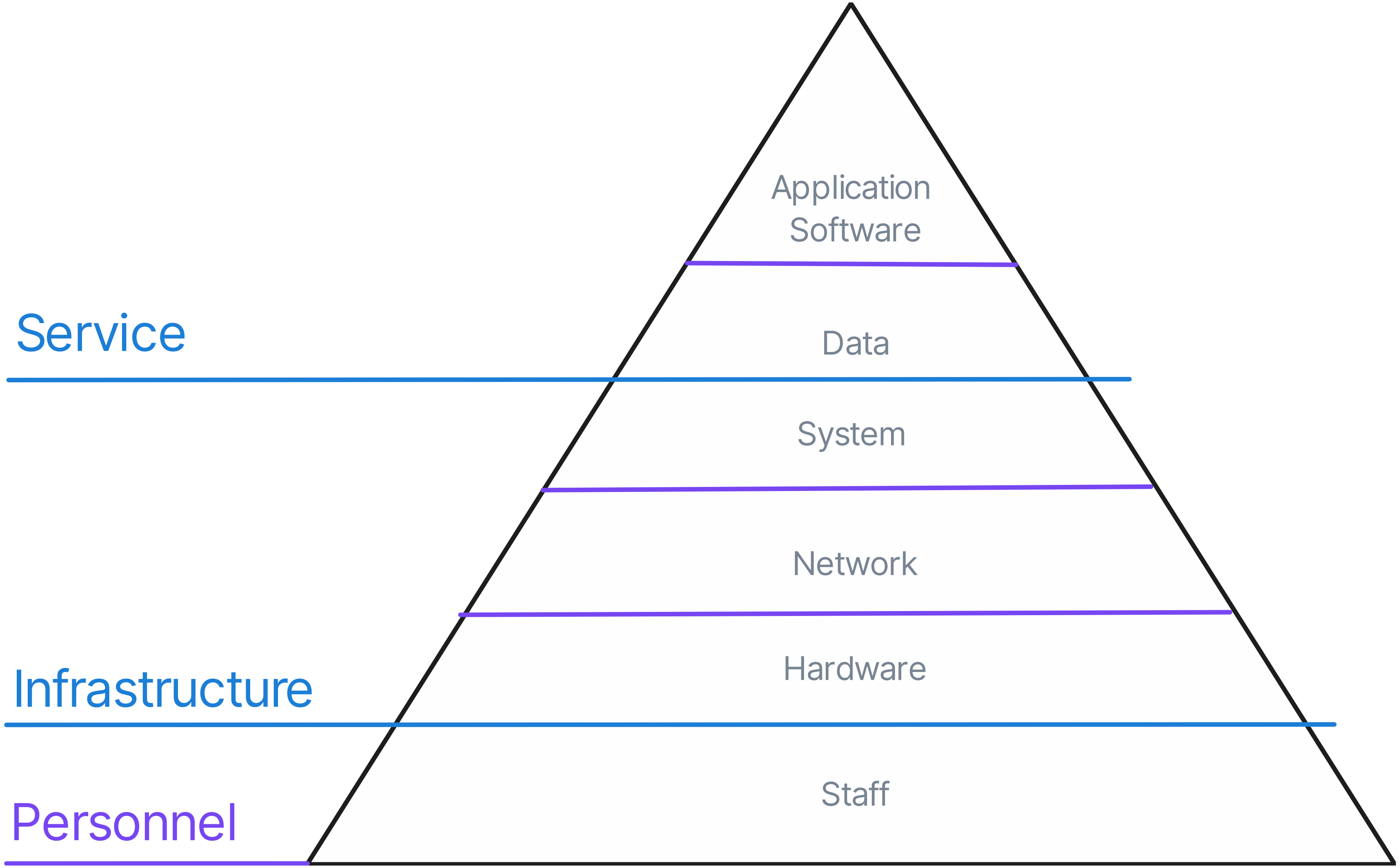
Models for Digital Resilience (a lot of related, but none specific)

CIA Model (Cybersecurity)

- Confidentiality
- Integrity
- Availability

CIA Model (Cybersecurity)

- Doesn't fit



還是倒機了

啊啊啊啊啊啊啊啊！

arrrgh!

CIA / Availability 互相包含

- CIA
  - Confidentiality
  - Integrity
  - Availability
- Availability
  - cybersecurity
  - accessibility
  - maintainability
  - etc, etc

啊啊啊啊啊！ **ARRRGH**！

ARRRGH

島在人在，島亡人亡

- Automation
- Redundancy
- Responsive
- Recovery
- Guidelines
- Hardening

(And Monitoring (C of PDCA))

CIA + Readiness (qualified, configured, and well-prepared)

Availability 換為 Accessibility

不只要在，還要存取得到

人（是否夠格）

資料（是否能直上）（backup 用 random 加密法，要靠通靈解密）

CIA + R

- Confidentiality
- Integrity
- Accessibility
- Readiness

CRAI / CIAR - 哭哭/賽啦

Digital Resilience Cheatsheet

Stack

- service
- application
- data
- system (online, backup)
- network
- infrastructure
- personnel

ARRRGH

- Automation
- Redundancy
- Responsive
- Recovery
- Guidelines
- Hardening

(And Monitoring (C of PDCA))

CRAI

- Confidentiality
- Integrity
- Accessibility
- Readiness

SRAAEE Model

- Security
  - Implement comprehensive security measures to protect data, software, networks, infrastructure, and services from threats. This includes technical, physical, and administrative measures.
- Redundancy and Recovery:
  - Maintain backup systems, data, and processes to avoid a single point of failure that could bring down the entire system. In the event of a security incident or other disruption, have efficient disaster recovery plans to restore services.
- Automation:
  - Incorporate technology to perform tasks with minimal human intervention. This can increase efficiency, reduce errors, and improve response times in areas such as security incident response, data backup, and system monitoring.
- Agility and Adaptation:
  - Cultivate a flexible and adaptable approach to system design and processes. This includes the ability to quickly adapt to changes and incorporate lessons learned from incidents, audits, and other experiences.
- Evaluation and Examination:
  - Regularly assess systems, processes, and personnel to identify potential vulnerabilities and areas for improvement. This also includes ongoing evaluation of the ever-changing threat environment, and regular testing of systems and disaster recovery plans.
- Education:
  - Regularly train and raise awareness among all personnel to ensure they understand their responsibilities in maintaining system security and resilience.

Other components

Vendor Management

Regulatory Compliance

Incident Response Planning

Business Continuity and Disaster Recovery Planning:

Digital Resilience Cheatsheet

Stack

- service
- application
- data
- system (online, backup)
- network
- infrastructure
- personnel

ARRRGH

- Automation
- Redundancy
- Responsive
- Recovery
- Guidelines
- Hardening

(And Monitoring (C of PDCA))

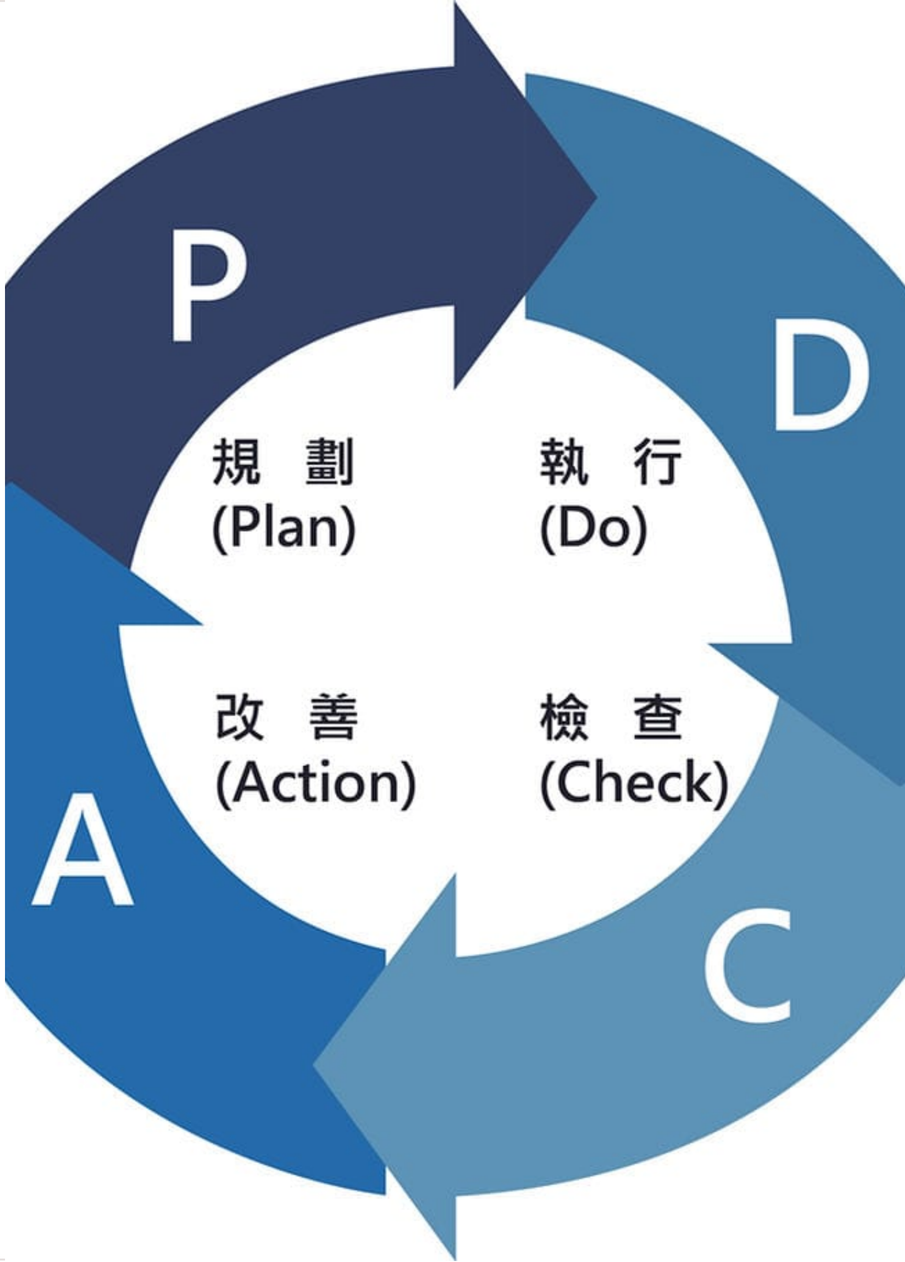
CRAI

- Confidentiality
- Integrity
- Accessibility
- Readiness

- Security
- Redundancy and Recovery
- Automation
- Agility and Adaptation
- Evaluation and Examination
- Education

PDCA

- Plan
- Do
- Check
- Act / Adjust



P/D: Risk Prevention and Control

- 風險控制：雞蛋不放同一個籃子。
    - 一次只讓一半承受風險
    - 團隊分別搭兩班不同飛機
    - k8s rolling update
- Isolation
    - network and env
    - 平時就在這種規劃的環境運行，遇到狀況不會擴散
    - kill switch / Backup plan
- Security/Exam data, infra, power, etc
- Scalability/Availability
- 需求管理與更變管理（Also A in PDCA）

C: Verifiability

- Monitoring
- 可驗證性
  - 例如，軟體的 SBOM（CycloneDX ）要有，才能驗證軟體及供應鏈的安全問題與穩定性等。
- 流程 - 整個都該是有韌性的
- CIA+R + 7 components + ARRRGH + SRAAEE
  - Scale up / scale out HA 沒有啟用
  - 只有一台設備，它倒機就全倒

驗證

1. what should be verified
2. what can be verified
3. what has been verified.

- services (user input/output)
- application (SAST/DAST).

Readiness in CRAI

使用某個產品，不代表相關功能有開啟、系統有設定好、有相關配合與能夠正確連動。

- 購買 WAF 但沒開功能
    - WAF 有裝，功能沒開，因為一開就撐不住，或是 DDoS 時 bypass
- 使用雲端但只是開一個 VM
    - 買了 LB 但沒設定好 service pool 或是後端伺服器根本沒法動態啟動服務

A: Maintainability and Modularity

- 需求管理與更變管理
- 可維護性
- 模組化
- 一坨義大利麵條 vs 權責分工
- Monolithic vs Microservice

Digital Resilience Cheatsheet

Stack

- service
- application
- data
- system (online, backup)
- network
- infrastructure
- personnel

ARRRGH

- Automation
- Redundancy
- Responsive
- Recovery
- Guidelines
- Hardening

(And Monitoring (C of PDCA))

CRAI

- Confidentiality
- Integrity
- Accessibility
- Readiness

- Security
- Redundancy and Recovery
- Automation
- Agility and Adaptation
- Evaluation and Examination
- Education

✓ □ PDCA

Mindset

Proactive, Reactive

Digital Resilience Cheatsheet

Stack

- service
- application
- data
- system (online, backup)
- network
- infrastructure
- personnel

ARRRGH

- Automation
- Redundancy
- Responsive
- Recovery
- Guidelines
- Hardening

(And Monitoring (C of PDCA))

CRAI

- Confidentiality
- Integrity
- Accessibility
- Readiness

- Security
- Redundancy and Recovery
- Automation
- Agility and Adaptation
- Evaluation and Examination
- Education

□ PDCA - Plan, Do, Check, Adjust

□ Mindset - Proactive, Reactive

轉

抉擇

Technology and Solution Selection

- 需求是什麼？ 使用量、對象、成本 然後綜合考量該做到哪、能做到哪
- 我們需要什麼能力、這個角色重要程度如何、這個角色使用頻率如何
- 成本（$、維護人力$、維護力可及度、維護力水準可及度/社群大小與文件完備度）（nginx/sws/lighttpd）
- Backup plan / fallback and rollback plan (url 資料庫失效時怎麼辦）
- 瞭解技術的特性、要解決的問題、有什麼限制

Standard Selection

- 「標準」的選擇
  - 檢視「標準」的特性
  - 例如 SPDX 與 CycloneDX 的差異性。

引用與解讀

法遵與標準

過時的、錯誤的引用與解讀。

Password

Password Requirements – GDPR, ISO 27001/27002, PCI DSS, NIST 800-53

NIST Special Publication 800-63B https://pages.nist.gov/800-63-3/sp800-63b.html

- 5.1.1.2 Memorized Secret

> Verifiers **SHOULD NOT** … **requiring mixtures of different character types** … Verifiers **SHOULD NOT require** memorized secrets to be **changed arbitrarily (e.g., periodically)**.

- Appendix A—Strength of Memorized Secrets
    - A.1 However, analyses of breached password databases reveal that the benefit of such rules is **not nearly as significant** as initially thought [Policies], although the **impact on usability and memorability is severe**.
    - A.2 Password **length** has been found to be a **primary factor** in characterizing password strength

Password

PCI DSS

- Requirement 8: Assign a unique ID to each person with computer access
  - 8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows
    - 8.1.4 Remove/disable inactive user accounts within 90 days. 2
  - 8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users:
    - 8.2.4 Change user passwords/passphrases at least once every 90 days. 2

合

Being solid, steady, calm, flexible, introspective, and constantly seeking progress

難打掛、不擴散、打掛也不怕

堅穩、踏實，
從容、靈活，
自省、求進。

設計堅固穩定，落實要確實，
應變方案妥善，反應要靈活，
持續檢核驗證，進步要持續。

Digital Resilience Cheatsheet

Stack

- service
- application
- data
- system (online, backup)
- network
- infrastructure
- personnel

ARRRGH

- Automation
- Redundancy
- Responsive
- Recovery
- Guidelines
- Hardening

(And Monitoring (C of PDCA))

CRAI

- Confidentiality
- Integrity
- Accessibility
- Readiness

- Security
- Redundancy and Recovery
- Automation
- Agility and Adaptation
- Evaluation and Examination
- Education

□ PDCA - Plan, Do, Check, Adjust

□ Mindset - Proactive, Reactive

也

巡航時的方法

檢驗一個系統：

- What do we know already (about the system)
- What we don't know yet (about the system)
- What might be missing (of the system)
- How to improve it. (Add or change)

What do we know (already)	What we don't know (yet)	What might be missing
How to improve it.		

Case study

- Physical or VM or container
- Isolation (runtime / system / network / infra (power outage infects backup circuits))
- Fix size or docker or docker swarm or k8s or ASG
- “Using AWS” 是否滿足 resilience (need multi AZ, ASG, etc)
- NIST 密碼規則建議（複雜度 vs 長度、更換頻率）
- 完整備份？差異備份？漸進備份?
    - RTO/RPO
- 快速部署（docker/container/ansible ）
- 機房 tier / 9s
- GitHub DDoS